Das Niedersächsische Datenschutzgesetz

Gesetzestext und Kommentar

Herausgeber
Der Landesbeauftragte
für den Datenschutz Niedersachsen
Joachim Wahlbrink
Brühlstraße 9, 30169 Hannover
Postfach 2 21, 30002 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599

E-Mail-Adresse poststelle@lfd.niedersachsen.de
Internet-Homepage http://www.lfd.niedersachsen.de

Stand: Dezember 2012

Inhaltsverzeichnis

	Seite
Vorwort	4
Abkürzungsverzeichnis	5
Einleitung	8
Text Niedersächsisches Datenschutzgesetz	11
Gesetzestext mit Kommentar	35
Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten	146
Verwaltungsvorschriften zum Niedersächsischen Datenschutzgesetz (VV NDSG)	147
Anlage 1 zu den VV NDSG: Verfahrensbeschreibung	167
Stichwortregister	170

Vorwort

Liebe Leserin, lieber Leser,

ich freue mich, Ihnen auf meiner Homepage die vierte Auflage dieser Broschüre zum Niedersächsischen Datenschutzgesetz mit der Kommentierung dieser Regelungen präsentieren zu können.

Die aktuelle Fassung enthält neben redaktionellen Änderungen datenschutzrechtliche Anpassungen, wie z. B. die Änderung der Rechtsstellung der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz sowie die Wiedereinführung des § 24 NDSG. Die Kommentierung soll Ihnen bei Fragestellungen im täglichen Umgang mit den Rechtsvorschriften dienen.

Ich hoffe, dass die Neuauflage der Broschüre Ihren Erwartungen gerecht wird. Für ergänzende Hinweise und Erfahrungsberichte bin ich auch zukünftig dankbar. Meine Mitarbeiterinnen und Mitarbeiter stehen Ihnen gern beratend zur Verfügung.

Ihr

Joachim Wahlbrink

Der Landesbeauftragte für den Datenschutz Niedersachsen

Abkürzungsverzeichnis

ABlEG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
AllGO	Verordnung über die Gebühren und Auslagen für Amtshandlungen und Leistungen - Allgemeine Gebührenordnung -
AO	Abgabenordnung
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BvR	Bundesverfassungsgericht (Abkürzung für Zitierung)
DIN	Deutsches Institut für Normung e. V.
DVBl.	Deutsches Verwaltungsblatt
EG	Europäische Gemeinschaft
EGStGB	Einführungsgesetz zum Strafgesetzbuch
EStG	Einkommensteuergesetz
EU	Europäische Union
GG	Grundgesetz
LfD Nds.	Landesbeauftragter für den Datenschutz Niedersachsen
LHO	Niedersächsische Landeshaushaltsordnung
LT-Drs.	Drucksache des Niedersächsischen Landtages –Landtags-Drucksache -
MI	Niedersächsisches Ministerium für Inneres, Sport und Integration
NAbfG	Niedersächsisches Abfallgesetz

NArchG	Gesetz über die Sicherung und Nutzung von Archivgut in Niedersachsen - Nds. Archivgesetz -
NBG	Niedersächsisches Beamtengesetz
NDSG	Niedersächsisches Datenschutzgesetz
NDiszG	Niedersächsisches Disziplinargesetz
Nds. GVBl.	Niedersächsisches Gesetz- und Verordnungsblatt
Nds. MBl.	Niedersächsisches Ministerialblatt
Nds. SOG	Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung
NHG	Niedersächsisches Hochschulgesetz
NJW	Neue Juristische Wochenschrift
NKomVG	Niedersächsisches Kommunalverfassungsgesetz
NKPG	Niedersächsisches Kommunalprüfungsgesetz
NMG	Niedersächsisches Meldegesetz
NPersVG	Niedersächsisches Personalvertretungsgesetz
NSchG	Niedersächsisches Schulgesetz
NStatG	Niedersächsisches Statistikgesetz
NVerfSchG	Gesetz über den Verfassungsschutz im Lande Niedersachsen
NVwKostG	Niedersächsisches Verwaltungskostengesetz
NVwVfG	Niedersächsisches Verwaltungsverfahrensgesetz
OWiG	Gesetz über Ordnungswidrigkeiten
PStG	Personenstandsgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StK	Niedersächsische Staatskanzlei
StPO	Strafprozessordnung
UWG	Gesetz gegen den unlauteren Wettbewerb
VV	Verwaltungsvorschriften
VV-Kor	Verwaltungsvorschrift zur Bekämpfung von Korruption in der Landesverwaltung
VwGO	Verwaltungsgerichtsordnung

VwKostG	Verwaltungskostengesetz
VwVfG	Verwaltungsverfahrensgesetz
ZustVO-OWi	Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten

Einleitung

Das Bundesverfassungsgericht hat mit Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz (BVerfGE 65,1) grundlegende Aussagen zum Datenschutz getroffen. Danach umfasst das Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1des Grundgesetzes) den Schutz des Einzelnen gegen eine unbegrenzte Erhebung, Speicherung, Weitergabe und Verwendung seiner Daten. Das Grundrecht gewährleistet die Befugnis, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dieses Recht bezeichnet das Bundesverfassungsgericht als **Recht auf informationelle Selbstbestimmung**.

Dieses Recht ist jedoch nicht schrankenlos. Die Gemeinschaftsbezogenheit des Einzelnen erfordert es, dass er Beschränkungen seines Rechts auf informationelle Selbstbestimmung hinnehmen muss. Solche Beschränkungen bedürfen nach den Feststellungen des Gerichts einer gesetzlichen Grundlage, die die Voraussetzungen und den Umfang dieser Beschränkungen erkennbar macht (**Grundsatz der Normenklarheit**). Außerdem ist der **Grundsatz der Verhältnismäßigkeit** zu beachten.

Da jede Datenverarbeitung einen Eingriff in das Persönlichkeitsrecht der Betroffenen darstellt, muss sie auf das unbedingt notwendige Maß beschränkt werden. Für die Verarbeitung personenbezogener Daten gilt deshalb der **Erforderlichkeitsgrundsatz**. Erforderlich ist eine Datenverarbeitung nur, wenn ohne sie eine Verwaltungsaufgabe nicht oder nicht sachgerecht erledigt werden kann (s. § 9).

Der Erforderlichkeitsgrundsatz wird durch den **Grundsatz der Zweckbindung** ergänzt. Er besagt, dass personenbezogene Daten von einer öffentlichen Stelle grundsätzlich nur für den Zweck verarbeitet werden dürfen, zu dem die Verwaltung die Daten erhalten hat. Damit wird vermieden, dass Daten, die jemand der Verwaltung für eine konkrete Verwaltungsaufgabe zur Verfügung gestellt hat, ohne sein Wissen in anderen Zusammenhängen verarbeitet werden.

Wer seine Rechte nach dem Datenschutzgesetz wahrnehmen will, muss in der Lage sein, die Verarbeitung seiner Daten zu überblicken. Das Bundesverfassungsgericht hebt deshalb die Bedeutung des **Transparenzgebot**s im Volkszählungsurteil besonders hervor. Nach seiner Formulierung müssen die Betroffenen wissen können, „wer was wann bei welcher Gelegenheit über ihn weiß“. Dies wird insbesondere durch das Recht auf Auskunft und Akteneinsicht gewährleistet.

Schließlich betont das Gericht die Bedeutung des vorbeugenden Datenschutzes, der z. B. durch technische oder organisatorische Verfahrensgestaltungen einer möglichen Rechtsbeeinträchtigung von vornherein entgegenwirkt.

Mit dem Niedersächsischen Datenschutzgesetz (NDSG) vom 17. Juni 1993 (Nds. GVBl. S. 141) hat der niedersächsische Gesetzgeber diese verfassungsrechtlichen Vorgaben umgesetzt und das bis dahin geltende Datenschutzgesetz aus dem Jahre 1978 abgelöst. Es folgten weitere Gesetzesänderungen:

- Artikel IV des Gesetzes zur Änderung des Vorläufigen Verwaltungsverfahrensgesetzes für das Land Niedersachsen und des Niedersächsischen Verwaltungsvollstreckungsgesetzes vom 29. Mai 1995 beinhaltete lediglich eine redaktionelle Änderung bei § 2 Abs. 6 NDSG.
- Im Jahre 1997 erfolgten mit dem Gesetz zur Änderung datenschutz-, gefahrenabwehr- und verwaltungsverfahrensrechtlicher Vorschriften vom 28. November 1997 sowie mit dem Dritten Gesetz zur Änderung dienstrechtlicher Vorschriften vom 17. Dezember 1997 diverse Rechtsänderungen des NDSG, u. a. zur automatisierten Datenverarbeitung.
- Durch das Gesetz zur Änderung des NDSG und zur Regelung der Berichtspflicht für Maßnahmen der Wohnraumüberwachung vom 21. Juni 2001 (Nds. GVBl. S. 373) wurde die Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie, ABlEG Nr. L281/31 vom 23. November 1995) umgesetzt. Ziele der Richtlinie sind, ein gleichwertiges Datenschutzniveau innerhalb der Europäischen Union (EU) zu gewährleisten, unterschiedliche Verfahrensregelungen zu harmonisieren und die Grundlage für einen freien und ungehinderten Datenverkehr zu schaffen.

  Die Regelungen der EG-Datenschutzrichtlinie gelten sowohl für die Datenverarbeitung durch die Wirtschaft (nicht öffentlicher Bereich) wie für die Datenverarbeitung durch öffentliche Stellen (öffentlicher Bereich). Mit dem am 6. Juli 2001 in Kraft getretenen Änderungsgesetz wurden u. a. folgende Rechtsänderungen eingefügt: Die Vorschrift über den behördlichen Datenschutzbeauftragten (§ 8 a), über automatisierte Einzelentscheidungen (§ 10 a), die Datenübermittlung ins Ausland (§ 14) und ein Widerspruchsrecht gegen die Datenverarbeitung (§ 17 a). Ferner hat der Gesetzgeber einige Neuregelungen aufgenommen, die nicht durch die Richtlinie vorgegeben sind, wie das **Gebot der Datensparsamkeit und Datenvermeidung** (§ 7 Abs. 4) und die Chipkartenregelung (§ 6 a). Das NDSG wurde in der Fassung vom 29. Januar 2002 neu bekannt gegeben.
- Im Dezember 2004 wurde mit Artikel 11 des Gesetzes zur Änderung des Niedersächsischen Verwaltungsverfahrensgesetzes und anderer Gesetze (Nds. GVBl. S. 634) § 25 a NDSG „Beobachtung durch Bildübertragung (Videoüberwachung)“ im NDSG eingefügt.
- In seiner Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht am 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - festgestellt, dass das allgemeine Persönlichkeitsrecht auch das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

- Im Juli 2011 wurden mit dem Gesetz zur Neuregelung der Rechtsstellung der oder des Landesbeauftragten für den Datenschutz (Nds. GVBl. S. 210, seit dem 08. Juli 2011 in Kraft getreten) die Forderungen des Europäischen Gerichtshofs (Urteil vom 09. März 2010 - C-518/07 -) zur Unanhängigkeit der Aufsichtsstellen für den Datenschutz mittels Änderung der Niedersächsischen Verfassung sowie des NDSG und weiterer Gesetze entsprochen.

Mit der vorliegenden Fassung des Gesetzes ist die Entwicklung des Datenschutzrechts selbstverständlich nicht abgeschlossen.

Unter den Datenschützern besteht Einigkeit, dass das geltende Datenschutzrecht die Zielvorstellungen der Transparenz, der Übersichtlichkeit und Verständlichkeit, der Angemessenheit der Problemlösungen und der Akzeptanz noch längst nicht hinreichend erfüllt und der Vollzug des Datenschutzes in seinen Strukturen verbessert werden muss. Insbesondere angesichts der rasant fortgeschrittenen technischen Entwicklungen und im Hinblick auf die mit der Nutzung des Internets verbundenen Probleme bedarf es dringend weitergehender materiell-rechtlicher, technischer und organisatorischer Regelungen.

Niedersächsisches Datenschutzgesetz (NDSG)

in der Fassung vom 29. Januar 2002 (Nds. GVBl. S. 22), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Dezember 2012 (Nds. GVBl. S. 589 - VORIS 20600 02 -)

Inhaltsübersicht

Erster Abschnitt

Allgemeine Bestimmungen

§ 1 Aufgabe des Gesetzes
§ 2 Anwendungsbereich
§ 3 Begriffsbestimmungen
§ 4 Zulässigkeit der Datenverarbeitung
§ 5 Datengeheimnis
§ 6 Verarbeitung personenbezogener Daten im Auftrag
§ 6 a Mobile personenbezogene Speicher- und Verarbeitungsmedien
§ 7 Technische und organisatorische Maßnahmen
§ 8 Verfahrensbeschreibung
§ 8 a Behördliche Datenschutzbeauftragte

Zweiter Abschnitt

Rechtsgrundlagen der Datenverarbeitung

§ 9 Erhebung
§ 10 Speicherung, Veränderung, Nutzung; Zweckbindung
§ 10 a Automatisierte Einzelentscheidung
§ 11 Übermittlung innerhalb des öffentlichen Bereichs
§ 12 Automatisiertes Abrufverfahren
§ 13 Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs
§ 14 Übermittlung an Personen oder Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums
§ 15 Übermittlung an Stellen öffentlich-rechtlicher Religionsgesellschaften

Dritter Abschnitt

Rechte der Betroffenen

§ 16 Auskunft, Einsicht in Akten
§ 17 Berichtigung, Löschung und Sperrung
§ 17 a Widerspruchsrecht
§ 18 Schadensersatz
§ 19 Anrufung der Landesbeauftragten oder des Landesbeauftragten
§ 20 Verzicht auf Rechte der Betroffenen

Vierter Abschnitt

Landesbeauftragte oder Landesbeauftragter für den Datenschutz

§ 21 Rechtsstellung der Landesbeauftragten oder des Landesbeauftragten
§ 21 a Disziplinarverfahren
§ 21 b Übertragung von Aufgaben
§ 22 Aufgaben, Rechte und Pflichten der Landesbeauftragten oder des Landesbeauftragten
§ 23 Beanstandungen durch die Landesbeauftragte oder den Landesbeauftragten

Fünfter Abschnitt

Besonderer Datenschutz

§ 24 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
§ 25 Verarbeitung personenbezogener Daten für Forschungsvorhaben
§ 25 a Beobachtung durch Bildübertragung
§ 26 Fernmessen und Fernwirken
§ 27 Öffentliche Auszeichnungen

Sechster Abschnitt

Übergangs- und Schlussvorschriften

§ 28 Straftaten
§ 29 Ordnungswidrigkeiten
§ 30 Übergangsvorschrift
§ 31 Aufhebung von Rechtsvorschriften
§ 32 Änderung des Niedersächsischen Meldegesetzes
§ 33 Änderung des Niedersächsischen Verfassungsschutzgesetzes
§ 34 In-Kraft-Treten

Erster Abschnitt

Allgemeine Bestimmungen

§ 1
Aufgabe des Gesetzes

[1]Aufgabe dieses Gesetzes ist es, das Recht einer jeden Person zu gewährleisten, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). [2]Dieses Gesetz bestimmt, unter welchen Voraussetzungen personenbezogene Daten durch öffentliche Stellen verarbeitet werden dürfen.

§ 2
Anwendungsbereich

(1) [1]Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen

1. des Landes,
2. der Gemeinden und Landkreise,
3. der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts

und deren Vereinigungen. [2]Sind einer Person oder Stelle außerhalb des öffentlichen Bereichs Aufgaben der öffentlichen Verwaltung übertragen, so ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(2) Der Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten und dabei die vom Landtag erlassene Datenschutzordnung anzuwenden haben.

(3) [1]Abweichend von Absatz 1 gelten nur die §§ 8, 19 und 26 sowie die Regelungen des Vierten Abschnitts, soweit personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeitet werden von

1. juristischen Personen des öffentlichen Rechts oder deren organisatorisch selbständigen Einrichtungen, die am Wettbewerb teilnehmen,
2. wirtschaftlichen Unternehmen der Gemeinden und Landkreise ohne eigene Rechtspersönlichkeit (Eigenbetriebe) und Zweckverbänden, die überwiegend wirtschaftliche Aufgaben wahrnehmen,
3. öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden.

[2]Für diese finden im Übrigen die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes in der Fassung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814), Anwendung.

(4) Auf öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen finden § 24 des Niedersächsischen Datenschutzgesetzes und im Übrigen die Vorschriften des Bundesdatenschutzgesetzes über nicht öffentliche Stellen Anwendung.

(5) Für öffentlich-rechtliche Rundfunkanstalten gilt das Recht des jeweiligen Sitzlandes.

(6) Besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten gehen den Bestimmungen dieses Gesetzes vor.

(7) Die Vorschriften dieses Gesetzes gehen denen des Niedersächsischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

(8) Auf das Gnadenverfahren findet dieses Gesetz mit Ausnahme des Vierten Abschnitts keine Anwendung.

§ 3
Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (Betroffene).

(2) [1]Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten. [2]Im Einzelnen ist

1. Erheben das Beschaffen von Daten über die Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,
3. Verändern das inhaltliche Umgestalten von Daten,
4. Übermitteln das Bekanntgeben von Daten an Dritte in der Weise, dass
   a) die Daten durch die Daten verarbeitende Stelle weitergegeben werden oder
   b) Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsehen oder abrufen,
5. Sperren das Kennzeichnen von Daten, um ihre weitere Verarbeitung einzuschränken,
6. Löschen das Unkenntlichmachen von Daten,
7. Nutzen jede sonstige Verwendung von Daten.

(3) Daten verarbeitende Stelle ist jede Stelle, die personenbezogene Daten selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt.

(4) [1]Empfänger ist jede Person oder Stelle, die Daten erhält. [2]Dritte sind Personen oder Stellen außerhalb der Daten verarbeitenden Stelle. [3]Dritte sind nicht die Betroffenen sowie diejenigen Personen und Stellen, die im Auftrag personenbezogene Daten verarbeiten (Auftragnehmer).

(5) Automatisierte Verarbeitung ist die Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

(6) [1]Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage und die Zusammenfassung solcher Unterlagen einschließlich der Bild- und Tonträger. [2]Hierunter fallen nicht Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

§ 4
Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. dieses Gesetz oder eine andere Rechtsvorschrift dies vorsieht oder
2. die Betroffenen eingewilligt haben.

(2) [1]Die Einwilligung bedarf der Schriftform, es sei denn, dass wegen besonderer Umstände eine andere Form angemessen ist. [2]Soweit die Einwilligung personenbezogene Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben betrifft, muss sie sich ausdrücklich auf diese Angaben beziehen. [3]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. [4]Die Betroffenen sind in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung auch über die Empfänger der Daten aufzuklären. [5]Die Betroffenen sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern oder mit Wirkung für die Zukunft widerrufen können.

(3) Die Einwilligung ist unwirksam, wenn sie durch Androhung rechtswidriger Nachteile oder durch Fehlen der Aufklärung bewirkt wurde.

§ 5
Datengeheimnis

Den Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, diese zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung ihrer Tätigkeit.

§ 6
Verarbeitung personenbezogener Daten im Auftrag

(1) [1]Werden personenbezogene Daten im Auftrag öffentlicher Stellen verarbeitet, so bleiben diese für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2]Die im Dritten Abschnitt genannten Rechte sind ihnen gegenüber geltend zu machen.

(2) [1]Die Auftragnehmer dürfen personenbezogene Daten nur im Rahmen der Weisungen der Auftraggeber verarbeiten. [2]Auftraggeber haben sich über die Beachtung der Maßnahmen nach § 7 und der erteilten Weisungen zu vergewissern.

(3) [1]Auftragnehmer müssen Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 7 bieten. [2]Aufträge, Weisungen zu technischen und

organisatorischen Maßnahmen und die Zulassung von Unterauftragsverhältnissen sind schriftlich festzuhalten.

(4) [1]Sofern die Vorschriften dieses Gesetzes auf Auftragnehmer keine Anwendung finden, hat die Daten verarbeitende Stelle den Auftragnehmer zu verpflichten, jederzeit vom Auftraggeber veranlasste Kontrollen zu ermöglichen. [2]Wird der Auftrag außerhalb des Geltungsbereichs dieses Gesetzes durchgeführt, so unterrichtet der Auftraggeber die zuständige Datenschutzkontrollbehörde.

§ 6 a
Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Stellen, die personenbezogene Speicher- und Verarbeitungsmedien herausgeben oder die auf solchen Medien Verfahren zur automatisierten Verarbeitung personenbezogener Daten aufbringen oder ändern, müssen die betroffene Person in allgemein verständlicher Form

1. über ihre Identität und Anschrift,
2. über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie die betroffene Person ihre Rechte nach den §§ 16 und 17 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit die oder der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichteten Stellen haben dafür Sorge zu tragen, dass die zur Wahrnehmung der Rechte nach den §§ 16 und 17 erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Die Tatsache der Kommunikation des mobilen personenbezogenen Speicher- und Verarbeitungsmediums muss für die betroffene Person eindeutig erkennbar sein.

§ 7
Technische und organisatorische Maßnahmen

(1) [1]Öffentliche Stellen haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung personenbezogener Daten sicherzustellen. [2]Der Aufwand für die Maßnahmen muss unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen.

(2) Werden personenbezogene Daten automatisiert verarbeitet, so sind Maßnahmen zu treffen, die je nach Art der Daten und ihrer Verwendung geeignet sind,

1. Unbefugten den Zugang zu den Verarbeitungsanlagen zu verwehren (Zugangskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit an wen übermittelt worden sind (Übermittlungskontrolle),
7. zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
9. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle),
10. zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
11. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) [1]Ein automatisiertes Verfahren darf nur eingesetzt oder wesentlich geändert werden, soweit Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien entstehen können, durch Maßnahmen nach Absatz 1 wirksam beherrscht werden können. [2]Die nach Satz 1 zu treffenden Feststellungen sind schriftlich festzuhalten.

(4) Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten.

(5) Personenbezogene Daten, die in Akten oder in anderer Weise ohne Einsatz automatisierter Verfahren verarbeitet werden, sind insbesondere vor dem Zugriff Unbefugter zu schützen.

§ 8
Verfahrensbeschreibung

[1]Jede öffentliche Stelle, die Verfahren zur automatisierten Verarbeitung personenbezogener Daten einrichtet oder ändert, hat in einer Beschreibung festzulegen:

1. die Bezeichnung der automatisierten Verarbeitung und ihre Zweckbestimmung,
2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,

3. den Kreis der Betroffenen,
4. die Art regelmäßig zu übermittelnder Daten, deren Empfänger, in den Fällen des § 6 auch die Auftragnehmer, sowie die Herkunft regelmäßig empfangener Daten,
5. die Absicht, Daten in Staaten nach § 14 zu übermitteln,
6. Fristen für die Sperrung und Löschung der Daten,
7. die technischen und organisatorischen Maßnahmen nach § 7,
8. die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

[2]Satz 1 gilt nicht, wenn die Daten nur vorübergehend und zu einem anderen Zweck als dem der inhaltlichen Auswertung gespeichert werden, sowie für Register nach § 8 a Abs. 4 und Verarbeitungen nach § 8 a Abs. 5 Satz 1.

§ 8 a
Behördliche Datenschutzbeauftragte

(1) [1]Jede öffentliche Stelle, die personenbezogene Daten automatisiert verarbeitet, hat eine Beauftragte oder einen Beauftragten für den Datenschutz zu bestellen. [2]Mit dieser Aufgabe kann auch eine Person beauftragt werden, die nicht der verarbeitenden Stelle angehört. [3]Ist die Person bereits von einer anderen Stelle zur Beauftragten für den Datenschutz bestellt worden, so setzt die weitere Bestellung das Einvernehmen mit der anderen Stelle voraus.

(2) [1]Bestellt werden darf nur, wer die erforderliche Sachkenntnis und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt mit anderen dienstlichen Aufgaben ausgesetzt ist. [2]Beauftragte sind in dieser Eigenschaft weisungsfrei; sie können sich unmittelbar an die Behördenleitung wenden und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. [3]Sie unterstützen die öffentliche Stelle bei der Sicherstellung des Datenschutzes und wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. [4]Sie sind über geplante Verfahren der automatisierten Verarbeitung personenbezogener Daten zu unterrichten. [5]Sie erhalten eine Übersicht der automatisierten Verarbeitungen mit den Angaben nach § 8 Satz 1. [6]Die öffentlichen Stellen haben die Beauftragten für den Datenschutz bei der Aufgabenerfüllung zu unterstützen.

(3) [1]Die Beauftragten haben auf Antrag die Angaben gemäß § 8 Satz 1 Nrn. 1 bis 6 jedermann in geeigneter Weise verfügbar zu machen. [2]Hiervon ausgenommen sind Beschreibungen nach § 22 Abs. 5 und Beschreibungen für Verarbeitungen zum Zweck der Strafverfolgung. [3]Den Beauftragten obliegt die Vorabprüfung von Verfahren nach § 7 Abs. 3, wobei in Zweifelsfällen die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz zu beteiligen ist. [4]Betroffene können sich unmittelbar an die Beauftragte oder den Beauftragten für den Datenschutz wenden.

(4) Wird in einer öffentlichen Stelle ein Register geführt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse geltend machen, zur Einsichtnahme offen

steht, so ist Absatz 1 nur anzuwenden, soweit in dieser öffentlichen Stelle andere automatisierte Verarbeitungen stattfinden.

(5) [1]Die Landesregierung wird ermächtigt, durch Verordnung die Pflicht zur Bestellung einer Beauftragten oder eines Beauftragten für den Datenschutz einzuschränken, soweit in einer öffentlichen Stelle automatisierte Verarbeitungen solche Daten betreffen, bei denen eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung nicht zu erwarten ist. [2]In der Verordnung sind die Zweckbestimmungen der Verarbeitung, die Kategorien der Daten, die Empfänger, denen die Daten übermittelt werden dürfen, und die Dauer der Aufbewahrung festzulegen.

Zweiter Abschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 9
Erhebung

(1)[1]Personenbezogene Daten dürfen erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. [2]Die Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. [3]Bei Dritten dürfen personenbezogene Daten nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. die Erhebung zur Abwehr von Gefahren für Leib, Leben oder die persönliche Freiheit erforderlich ist,
3. Angaben der Betroffenen überprüft werden müssen,
4. offensichtlich ist, dass die Erhebung im Interesse der Betroffenen liegt und sie einwilligen würden,
5. die Daten aus allgemein zugänglichen Quellen entnommen werden können, soweit nicht schutzwürdige Interessen der Betroffenen offensichtlich entgegenstehen, oder
6. a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

   b) die Erhebung bei den Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

(2) [1]Werden Daten bei den Betroffenen erhoben, so sind sie über den Zweck der Erhebung aufzuklären. [2]Werden die Daten aufgrund einer Rechtsvorschrift erhoben, so sind die Betroffenen in geeigneter Weise über diese aufzuklären. [3]Soweit eine Auskunftspflicht besteht oder die Gewährung von Rechtsvorteilen die Angabe von Daten voraussetzt, sind die Betroffenen hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(3) [1]Werden Daten bei einer dritten Person oder einer Stelle außerhalb des öffentlichen Bereichs erhoben, so ist diese auf Verlangen über den Verwendungszweck

aufzuklären. [2]Soweit eine Auskunftspflicht besteht, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 10
Speicherung, Veränderung, Nutzung; Zweckbindung

(1) [1]Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und die Daten für diese Zwecke erhoben worden sind. [2]Erlangt die öffentliche Stelle Kenntnis von personenbezogenen Daten, ohne diese erhoben zu haben, so darf sie diese Daten nur für Zwecke verarbeiten, für die sie diese Daten erstmals speichert.

(2) [1]Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig,

1. wenn die Betroffenen eingewilligt haben,
2. in den Fällen des § 9 Abs. 1 Satz 3 Nrn. 1 bis 5 oder
3. wenn sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten ist.

[2]Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, so dürfen sie für andere Zwecke nur gespeichert, verändert oder genutzt werden, wenn die Betroffenen eingewilligt haben oder wenn eine Rechtsvorschrift dies zulässt.

(3) [1]Ein Speichern, Verändern oder Nutzen zu anderen Zwecken liegt nicht vor, wenn dies zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen erfolgt. [2]Zulässig ist auch die Verarbeitung zu Ausbildungs- und Prüfungszwecken, soweit nicht berechtigte Interessen der Betroffenen an der Geheimhaltung der Daten offensichtlich überwiegen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verarbeitet werden.

§ 10 a
Automatisierte Einzelentscheidung

(1) Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

(2) [1]Dies gilt nicht, wenn

1. eine Rechtsvorschrift dies vorsieht,
2. dem Begehren der Betroffenen stattgegeben wurde oder

3. die Wahrung der berechtigten Interessen der Betroffenen durch geeignete Maßnahmen gewährleistet und den Betroffenen von der verantwortlichen Stelle die Tatsache, dass eine Entscheidung nach Absatz 1 vorliegt, mitgeteilt wird.

[2]Als geeignete Maßnahme im Sinne der Nummer 3 gilt insbesondere die Möglichkeit der Betroffenen, ihren Standpunkt geltend zu machen; die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

(3) Das Recht der Betroffenen auf Auskunft nach § 16 erstreckt sich in den Fällen des Absatzes 1 auch auf den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten.

§ 11
Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nur zulässig, wenn die Übermittlung zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen.

(2) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten der Betroffenen oder Dritter in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der Betroffenen oder Dritter an deren Geheimhaltung offensichtlich überwiegen; eine weitere Verarbeitung dieser Daten ist unzulässig.

(3) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. [2]Erfolgt die Übermittlung aufgrund eines Ersuchens, so hat die übermittelnde Stelle lediglich zu prüfen, ob sich das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden Stelle hält. [3]Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; die empfangende Stelle hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. [4]Erfolgt die Übermittlung durch automatisierten Abruf (§ 12), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs die empfangende Stelle.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 12
Automatisiertes Abrufverfahren

(1) [1]Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf eines Dritten ermöglicht, darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies zulässt. [2]Die Zulässigkeit des einzelnen Abrufs bestimmt sich nach den Vorschriften dieses Gesetzes.

(2) [1]Die Landesregierung wird ermächtigt, durch Verordnung für die Behörden und Einrichtungen des Landes sowie für die der Aufsicht des Landes unterliegenden sonstigen öffentlichen Stellen die Einrichtung automatischer Abrufverfahren zuzulassen. [2]Für die Zulassung solcher Verfahren innerhalb des Geschäftsbereichs eines

Ministeriums wird das jeweilige Ministerium ermächtigt, die Verordnung zu erlassen. [3]Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung der schutzwürdigen Interessen des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. [4]In der Verordnung sind die Datenempfänger, die Art der zu übermittelnden Daten, der Zweck des Abrufs sowie die wesentlichen bei den beteiligten Stellen zu treffenden Maßnahmen zur Kontrolle der Verarbeitung festzulegen. [5]Die Landesbeauftragte für den Datenschutz oder der Landesbeauftragte für den Datenschutz (die Landesbeauftragte oder der Landesbeauftragte) ist vorher zu hören.

(3) Sind automatisierte Abrufverfahren in einer Verordnung nach Absatz 2 zugelassen, so dürfen sie auf Verlangen des Landesrechnungshofs auch für die Rechnungsprüfung eingesetzt werden.

(4) [1]Personenbezogene Daten dürfen nicht zum Abruf durch Personen oder Stellen außerhalb des öffentlichen Bereichs bereitgehalten werden. [2]Dies gilt nicht für den Abruf durch Betroffene.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus solchen Datenbeständen, die jeder Person offen stehen oder deren Inhalt veröffentlicht werden darf.

§ 13
Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) [1]Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen,
2. die Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt, oder
3. sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben.

[2]In den Fällen des Satzes 1 Nr. 3 sind die Betroffenen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten.

(2) Die übermittelnde Stelle hat die Empfänger zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie ihnen übermittelt wurden.

§ 14
Übermittlung an Personen oder Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums

(1) [1]Die Übermittlung personenbezogener Daten an Personen und Stellen in Staaten außerhalb der Europäischen Union und der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sowie an über- und zwischenstaatliche Stellen ist

zulässig, soweit die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaften oder einem internationalen Vertrag geregelt ist. [2]Eine Übermittlung an öffentliche Stellen darf auch erfolgen, wenn die Voraussetzungen des § 11 Abs. 1 sowie an andere Empfänger, wenn die Voraussetzungen des § 13 Abs. 1 erfüllt sind und im Empfängerland gleichwertige Datenschutzregelungen gelten. [3]Die Übermittlung nach Satz 2 darf nicht erfolgen, soweit Grund zu der Annahme besteht, dass die Übermittlung einen Verstoß gegen wesentliche Grundsätze des deutschen Rechts, insbesondere gegen Grundrechte, zur Folge haben würde.

(2) Eine Übermittlung ist abweichend von Absatz 1 Satz 2 auch dann zulässig, wenn sie

1. für die Wahrnehmung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
2. für die Wahrung lebenswichtiger Interessen der Betroffenen erforderlich ist oder
3. aus einem Register erfolgt,

   a) das zur Information der Öffentlichkeit bestimmt ist oder

   b) in das alle Personen, die ein berechtigtes Interesse an der Einsichtnahme haben, Einsicht nehmen können,

   soweit der ausländische Empfänger die Voraussetzungen für die Einsichtnahme erfüllt.

§ 15
Übermittlung an Stellen öffentlich-rechtlicher Religionsgesellschaften

[1]Die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften ist zulässig, wenn

1. die Betroffenen eingewilligt haben,
2. eine Rechtsvorschrift dies vorsieht,
3. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen,
4. offensichtlich ist, dass die Übermittlung im Interesse der Betroffenen liegt und sie einwilligen würden, oder
5. sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben

und sichergestellt ist, dass bei den Empfängern ausreichende Datenschutzmaßnahmen, insbesondere Regelungen zur Zweckbindung, getroffen sind. [2]In den Fällen des Satzes 1 Nr. 5 sind die Betroffenen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten.

Dritter Abschnitt
Rechte der Betroffenen

§ 16
Auskunft, Einsicht in Akten

(1) [1]Betroffenen ist von der Daten verarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung,
3. die Herkunft der Daten, die Empfänger von Übermittlungen, in den Fällen des § 6 auch die Auftragnehmer, sowie
4. in den Fällen des § 10 a über die Art und Struktur der automatisierten Verarbeitung.

[2]Dies gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. [3]Für gesperrte Daten, die nur deshalb noch gespeichert sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, gilt die Verpflichtung zur Auskunftserteilung nur, wenn Betroffene ein berechtigtes Interesse an der Erteilung der Auskunft über diese Daten glaubhaft machen.

(2) [1]In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnet werden. [2]Die Daten verarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(3) Sind die Daten in Akten gespeichert, so können Betroffene Auskunft aus Akten oder Akteneinsicht verlangen, soweit sie Angaben machen, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen.

(4) Anträge nach Absatz 1 oder 3 können abgelehnt werden, soweit und solange

1. die Erfüllung des Auskunfts- oder Einsichtsverlangens die ordnungsgemäße Wahrnehmung der übrigen Aufgaben der datenverarbeitenden Stelle gefährden würde,
2. die Auskunft oder Einsicht die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen von Dritten geheim zu halten sind.

(5) [1]Die Ablehnung der Auskunft oder der Akteneinsicht bedarf keiner Begründung, soweit durch die Begründung der Zweck der Ablehnung gefährdet würde. [2]Die Gründe der Ablehnung sind aktenkundig zu machen.

(6) Wird die Auskunft oder die Akteneinsicht abgelehnt, so sind die Betroffenen darauf hinzuweisen, dass sie sich an die Landesbeauftragte oder den Landesbeauftragten wenden können.

(7) Auskunft und Akteneinsicht sind kostenfrei.

§ 17
Berichtigung, Löschung und Sperrung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) [1]Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

[2]In den Fällen des Satzes 1 Nr. 2 tritt an die Stelle der Löschung die Abgabe an das zuständige Archiv, soweit dies in den entsprechenden Rechtsvorschriften vorgesehen ist. [3]Sind personenbezogene Daten in Akten gespeichert, so ist die Löschung nach Satz 1 Nr. 2 durchzuführen, wenn die gesamte Akte nach Maßgabe der entsprechenden Rechts- oder Verwaltungsvorschriften zur Aufgabenerfüllung nicht mehr erforderlich ist. [4]Werden durch die weitere Speicherung nach Satz 3 schutzwürdige Belange der Betroffenen erheblich beeinträchtigt, so sind die entsprechenden Daten zu sperren.

(3) [1]Personenbezogene Daten sind zu sperren,

1. solange und soweit ihre Richtigkeit von den Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
2. wenn die Betroffenen anstelle der Löschung unzulässig gespeicherter Daten die Sperrung verlangen oder die weitere Speicherung im Interesse der Betroffenen geboten ist, oder
3. solange sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen.

[2]Gesperrte Daten sind mit einem Sperrvermerk zu versehen; in automatisierten Verfahren ist die Sperrung durch zusätzliche technische Maßnahmen zu gewährleisten. [3]Gesperrte Daten dürfen nicht mehr weiter verarbeitet werden, es sei denn, dass dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder Dritter liegenden Gründen unerlässlich ist oder die Betroffenen eingewilligt haben. [4]Die Gründe für die Verarbeitung gesperrter Daten sind aufzuzeichnen.

(4) [1]Sind Daten nach den Absätzen 1 bis 3 berichtigt, gesperrt oder gelöscht worden, so sind die Personen oder Stellen unverzüglich zu unterrichten, denen die Daten übermittelt worden sind. [2]Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden.

§ 17 a
Widerspruchsrecht

[1]Betroffene haben gegenüber der Daten verarbeitenden Stelle das Recht, der Verarbeitung der sie betreffenden Daten aus schutzwürdigen persönlichen Gründen zu widersprechen. [2]Soweit diese Gründe überwiegen, ist die Verarbeitung der Daten unzulässig. [3]Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 18
Schadensersatz

(1) [1]Wird den Betroffenen durch eine nach datenschutzrechtlichen Vorschriften unzulässige Verarbeitung ihrer personenbezogenen Daten ein Schaden zugefügt, so sind ihnen die Träger der Daten verarbeitenden Stellen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet; im Fall einer nicht automatisierten Verarbeitung besteht die Ersatzpflicht nicht, wenn die Daten verarbeitende Stelle nachweist, dass die Unzulässigkeit nicht von ihr zu vertreten ist. [2]Bei einer schweren Verletzung des Persönlichkeitsrechts kann auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangt werden. [3]Ersatzpflichtige haften gegenüber jeder betroffenen Person für jedes schädigende Ereignis bis zu einem Betrag von 250 000 Euro. Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(2) Auf ein Mitverschulden der Betroffenen ist § 254 und auf die Verjährung des Schadensersatzanspruchs § 199 Abs. 3 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

§ 19
Anrufung der Landesbeauftragten oder des Landesbeauftragten

(1) [1]Jede Person, die meint, durch die Verarbeitung ihrer personenbezogenen Daten in ihren Rechten durch eine Stelle verletzt worden zu sein, die der Kontrolle nach den Vorschriften dieses Gesetzes unterliegt, kann sich an die Landesbeauftragte oder den Landesbeauftragten wenden. [2]Keine Person darf deswegen benachteiligt werden.

(2) [1]Die Bediensteten der Behörden und sonstigen öffentlichen Stellen, auf die dieses Gesetz Anwendung findet, dürfen sich unbeschadet ihres Rechts nach Absatz 1 in allen Angelegenheiten des Datenschutzes jederzeit an die Landesbeauftragte oder den Landesbeauftragten wenden. [2]Der Einhaltung des Dienstweges bedarf es nicht, wenn die Bedienstete oder der Bedienstete auf einen Verstoß gegen datenschutzrechtliche Vorschriften oder auf die Gefahr hingewiesen hat, dass eine Person in unzulässiger Weise in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt wird, und diesem Hinweis binnen angemessener Frist nicht abgeholfen worden ist. [3]Im Übrigen bleiben die dienstrechtlichen Pflichten der Bediensteten unberührt.

§ 20
Verzicht auf Rechte der Betroffenen

Die in diesem Abschnitt genannten Rechte können auch durch die Einwilligung der Betroffenen nicht im Voraus ausgeschlossen oder beschränkt werden.

Vierter Abschnitt
Landesbeauftragte oder Landesbeauftragter für den Datenschutz

§ 21
Rechtsstellung der Landesbeauftragten oder des Landesbeauftragten

(1) [1]Die Landesbeauftragte oder der Landesbeauftragte soll die Befähigung zum Richteramt haben. [2]Sie oder er wird nach der Wahl durch den Landtag auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen. [3]Die Wiederwahl und die Berufung für eine weitere Amtszeit sind zulässig. [4]Das Amt ist im Übrigen bis zum Eintritt der Nachfolge weiterzuführen. [5]Die Landesbeauftragte oder der Landesbeauftragte kann außer auf Antrag nur entlassen werden, wenn der Pflicht nach Satz 4 nicht nachgekommen wird oder wenn Gründe vorliegen, die bei einem Richterverhältnis auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

(2) [1]Für die Landesbeauftragte oder den Landesbeauftragten gilt keine Altersgrenze. [2]§ 37 des Niedersächsischen Beamtengesetzes ist nicht anzuwenden.

(3) [1]Die Landesbeauftragte oder der Landesbeauftragte ist Leiterin oder Leiter einer von der Landesregierung unabhängigen obersten Landesbehörde mit Sitz in Hannover. [2]Soweit dienstrechtliche Befugnisse der Landesregierung zustehen, werden Stellen auf Vorschlag der Landesbeauftragten oder des Landesbeauftragten besetzt. [3]Die Bediensteten können ohne ihre Zustimmung nur im Einvernehmen mit der Landesbeauftragten oder dem Landesbeauftragten versetzt, abgeordnet oder umgesetzt werden.

§ 21 a
Disziplinarverfahren

(1) In Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten gelten die Vorschriften des Niedersächsischen Disziplinargesetzes nach Maßgabe der folgenden Absätze.

(2) [1]Für Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten ist der Niedersächsische Dienstgerichtshof für Richter (Dienstgerichtshof) zuständig. [2]Entscheidungen des Dienstgerichtshofs im Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten werden mit der Verkündung oder der sie ersetzenden Zustellung rechtskräftig.[3]Der Dienstgerichtshof entscheidet auf Antrag der Präsidentin oder des Präsidenten des Landtages.

(3) [1]Der Verweis ist als Disziplinarmaßnahme ausgeschlossen. [2]Über die vorläufige Dienstenthebung und die Einbehaltung von Dienstbezügen sowie über die Aufhebung dieser Maßnahmen entscheidet auf Antrag der Präsidentin oder des Präsidenten des Landtages der Dienstgerichtshof durch Beschluss.

(4) [1]Die nicht ständigen Mitglieder des Dienstgerichtshofs müssen der Verwaltungsgerichtsbarkeit angehören. [2]Auf die Besetzung des Dienstgerichtshofs finden im Übrigen die §§ 81 bis 83, 86 Abs. 2 Satz 1 und Abs. 4 und 5 sowie die §§ 87 und 88 des Niedersächsischen Richtergesetzes entsprechende Anwendung.

§ 21 b
Übertragung von Aufgaben

Überträgt die Landesbeauftragte oder der Landesbeauftragte Aufgaben der Personalverwaltung ganz oder teilweise auf eine andere Behörde, so dürfen personenbezogene Daten aus der Personalakte auch ohne Einwilligung der oder des Betroffenen an diese Behörde übermittelt und von ihr verarbeitet werden, soweit dies für die Erfüllung der übertragenen Aufgabe erforderlich ist.

§ 22
Aufgaben, Rechte und Pflichten der Landesbeauftragten oder des Landesbeauftragten

(1) [1]Die Landesbeauftragte oder der Landesbeauftragte kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen. [2]Der Landtag, die Gerichte und der Landesrechnungshof unterliegen dieser Kontrolle aber nur, soweit sie in Verwaltungsangelegenheiten tätig werden. [3]Außerdem kann die Landesbeauftragte oder der Landesbeauftragte den Landtag, die Landesregierung, die übrigen Behörden und sonstigen öffentlichen Stellen über Verbesserungen des Datenschutzes beraten. [4]Die Landesbeauftragte oder der Landesbeauftragte ist bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften anzuhören, die Regelungen zum Recht auf informationelle Selbstbestimmung zum Gegenstand haben.

(2) Die Landesbeauftragte oder der Landesbeauftragte ist rechtzeitig über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme zu unterrichten.

(3) [1]Die Landesbeauftragte oder der Landesbeauftragte legt dem Landtag jeweils für zwei Kalenderjahre einen Tätigkeitsbericht vor. [2]Die Landesregierung nimmt hierzu gegenüber dem Landtag innerhalb von sechs Monaten Stellung. [3] Die Landesbeauftragte oder der Landesbeauftragte unterrichtet den Landtag und die Öffentlichkeit auch über wesentliche Entwicklungen des Datenschutzes. [4]Auf Ersuchen des Landtages, seines zuständigen Ausschusses oder der Landesregierung hat die Landesbeauftragte oder der Landesbeauftragte ferner Angelegenheiten von besonderer datenschutzrechtlicher Bedeutung zu untersuchen und über die Ergebnisse zu berichten. [5]Die Landesbeauftragte oder der Landesbeauftragte hat in bedeutsamen Fällen alsbald dem Landtag schriftlich oder in den Sitzungen seiner Ausschüsse mündlich zu berichten. [6]Auf Ersuchen des Landtages oder seines zuständigen

Ausschusses hat die Landesbeauftragte oder der Landesbeauftragte auch in sonstigen Fällen über einzelne Vorgänge aus ihrem oder seinem Tätigkeitsbereich zu berichten und auf Ersuchen dazu Akten vorzulegen. [7]Die Landesbeauftragte oder der Landesbeauftragte braucht Ersuchen nach Satz 6 nicht zu entsprechen, soweit dadurch ihre oder seine Funktionsfähigkeit wesentlich beeinträchtigt würde. [8]Schriftliche Äußerungen gegenüber dem Landtag sind gleichzeitig der Landesregierung vorzulegen.

(4) [1]Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten bei der Erfüllung der Aufgaben zu unterstützen. [2]Dazu haben sie insbesondere

1. Auskunft zu erteilen sowie Einsicht in alle Unterlagen zu gewähren, die die Landesbeauftragte oder der Landesbeauftragte zur Erfüllung der Aufgaben für erforderlich hält,

2. die in Nummer 1 genannten Unterlagen auf Verlangen innerhalb einer bestimmten Frist zu übersenden,

3. jederzeit Zutritt in alle Diensträume zu gewähren.

[3]Die oberste Landesbehörde entscheidet, ob der Landesbeauftragten oder dem Landesbeauftragten personenbezogene Daten einer betroffenen Person zu offenbaren sind, wenn dieser Vertraulichkeit besonders zugesichert worden ist.

(5) Beschreibungen nach § 8 sind der Landesbeauftragten oder dem Landesbeauftragten zu übersenden, wenn die Verarbeitungen zur Erfüllung

1. der Aufgaben nach dem Niedersächsischen Verfassungsschutzgesetz oder

2. polizeilicher Aufgaben nach dem Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG) erfolgen.

(6) [1]Die Landesbeauftragte oder der Landesbeauftragte ist auch Aufsichtsbehörde im Sinne des § 38 des Bundesdatenschutzgesetzes für die Kontrolle der Durchführung des Datenschutzes bei der Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen. [2]Absatz 3 Sätze 1, 3 und 5 bis 7 gilt entsprechend.

§ 23
Beanstandungen durch die Landesbeauftragte oder den Landesbeauftragten

(1) [1]Stellt die Landesbeauftragte oder der Landesbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen fest, so ist dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,

2. bei den Gemeinden, Landkreisen und den sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem vertretungsberechtigten Organ

mit der Aufforderung zu beanstanden, innerhalb einer bestimmten Frist Stellung zu nehmen. [2]In den Fällen des Satzes 1 Nr. 2 ist gleichzeitig auch die zuständige Aufsichtsbehörde zu unterrichten.

(2) [1]Die Stellungnahme soll auch die Maßnahmen darstellen, die der Beanstandung abhelfen sollen. [2]Die in Absatz 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme zu.

(3) Die Landesbeauftragte oder der Landesbeauftragte kann insbesondere dann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt oder die Beseitigung der Mängel sichergestellt ist.

Fünfter Abschnitt
Besonderer Datenschutz

§ 24

Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Die beamtenrechtlichen Vorschriften über die Führung von Personalakten gemäß § 50 des Beamtenstatusgesetzes und §§ 88 bis 95 des Niedersächsischen Beamtengesetzes sind für alle nicht beamteten Beschäftigten einer öffentlichen Stelle entsprechend anzuwenden, soweit tarifvertraglich nichts anderes geregelt ist.

(2) [1]Werden Feststellungen über die Eignung einer Bewerberin oder eines Bewerbers für ein Dienstverhältnis durch ärztliche oder psychologische Untersuchungen oder Tests getroffen, so darf die Einstellungsbehörde von der untersuchenden Person oder Stelle in der Regel nur das Ergebnis der Eignungsuntersuchung und solche Feststellungen anfordern, die die gesundheitliche Eignung beeinträchtigen könne (Risikofaktoren). [2]Weitere personenbezogene Daten darf sie nur anfordern, wenn sie die Bewerberin oder den Bewerber zuvor schriftlich über die Gründe dafür unterrichtet hat. [3]Die Weiterverarbeitung der übermittelten und gespeicherten Daten ist nur mit schriftlicher Einwilligung der Bewerberin oder des Bewerbers zulässig.

§ 25
Verarbeitung personenbezogener Daten für Forschungsvorhaben

(1) Für die Verarbeitung personenbezogener Daten zur Durchführung von wissenschaftlichen Forschungsvorhaben sind die §§ 9 bis 15 nach Maßgabe der Absätze 2 bis 5 und 7 anzuwenden.

(2) Für wissenschaftliche Forschungsvorhaben dürfen personenbezogene Daten, die für andere Zwecke oder für ein anderes Forschungsvorhaben erhoben oder gespeichert worden sind, verarbeitet werden, wenn

1. die Betroffenen eingewilligt haben,
2. eine Rechtsvorschrift dies vorsieht oder
3. Art und Verarbeitung der Daten darauf schließen lassen, dass ein schutzwürdiges Interesse der Betroffenen der Verarbeitung der Daten für das Forschungsvorhaben nicht entgegensteht oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der Betroffenen erheblich überwiegt. Das Ergebnis der Abwägung und seine Begründung sind aufzuzeichnen. Über die Verarbeitung ist die Datenschutzbeauftragte oder der Datenschutzbeauftragte nach § 8 a zu unterrichten.

(3) Die für ein Forschungsvorhaben gespeicherten oder übermittelten Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.

(4) Sobald der Stand des Forschungsvorhabens es gestattet, sind die Merkmale, mit deren Hilfe ein Bezug auf eine bestimmte natürliche Person hergestellt werden kann, gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck dies gestattet.

(5) Im Rahmen von wissenschaftlichen Forschungsvorhaben dürfen personenbezogene Daten nur veröffentlicht werden, wenn

1. die Betroffenen eingewilligt haben oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(6) Die Einwilligung der Betroffenen bedarf nicht der Schriftform, wenn hierdurch das Forschungsvorhaben erheblich beeinträchtigt würde.

(7) [1]Eine Übermittlung personenbezogener Daten an Empfänger, auf die dieses Gesetz keine Anwendung findet, ist nach Maßgabe des Absatzes 2 zulässig, wenn sich die Empfänger verpflichten, die Daten nur für das von ihnen zu bezeichnende Forschungsvorhaben und nach Maßgabe der Absätze 3 bis 5 zu verarbeiten. [2]Die Übermittlung ist der Landesbeauftragten oder dem Landesbeauftragten rechtzeitig vorher anzuzeigen.

§ 25 a
Beobachtung durch Bildübertragung

(1) Die Beobachtung öffentlich zugänglicher Räume durch Bildübertragung (Videoüberwachung) ist nur zulässig, soweit sie

1. zum Schutz von Personen, die der beobachtenden Stelle angehören oder diese aufsuchen, oder
2. zum Schutz von Sachen, die zu der beobachtenden Stelle oder zu den Personen nach Nummer 1 gehören,

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der von der Beobachtung betroffenen Personen überwiegen.

(2) [1]Die Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder die Betroffenen ausdrücklich eingewilligt haben.

(3) Die Möglichkeiten der Beobachtung und der Aufzeichnung sowie die verarbeitende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(4) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese über die jeweilige Verarbeitung zu unterrichten. [2]Von einer Unterrichtung kann abgesehen werden,

1. solange das öffentliche Interesse an einer Strafverfolgung das Unterrichtungsrecht der betroffenen Person erheblich überwiegt oder
2. wenn die Unterrichtung im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

(6) Dem Einsatz der Videoüberwachung muss stets eine Prüfung nach § 7 Abs. 3 vorausgehen.

§ 26
Fernmessen und Fernwirken

(1) [1]Ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) dürfen in Wohnungen oder Geschäftsräumen nur vorgenommen werden, wenn die Betroffenen zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden sind und nach der Unterrichtung schriftlich eingewilligt haben. [2]Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen Wirkungen auszulösen (Fernwirkdienste). [3]Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn die Betroffenen erkennen können, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist. [4]Die Betroffenen können ihre Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. [5]Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) [1]Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht von der Einwilligung nach Absatz 1 abhängig gemacht werden. [2]Betroffenen dürfen keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen, wenn sie ihre Einwilligung verweigern oder widerrufen.

(3) [1]Die im Rahmen von Fernmess- oder Fernwirkdiensten erhobenen Daten dürfen nur zu den vereinbarten Zwecken verarbeitet werden. [2]Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 27
Öffentliche Auszeichnungen

(1) [1]Zur Vorbereitung öffentlicher Auszeichnungen dürfen die dazu erforderlichen personenbezogenen Daten auch ohne Kenntnis der Betroffenen bei anderen Personen oder Stellen erhoben werden. [2]Auf Anforderung dürfen öffentliche Stellen die erforderlichen Daten übermitteln.

(2) § 16 findet keine Anwendung.

Sechster Abschnitt
Übergangs- und Schlussvorschriften

§ 28
Straftaten

(1) [1]Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten, die nicht allgemein zugänglich sind,

1. unbefugt erhebt, speichert, verändert, löscht, übermittelt oder nutzt oder
2. durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Der Versuch ist strafbar.

§ 29
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. entgegen § 5 zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeitet oder offenbart oder
2. sich durch Vortäuschung falscher Tatsachen verschafft oder an sich oder andere übermitteln lässt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden.

§§ 30 bis 34

Vom Abdruck der §§

30 (Übergangsvorschrift)

31 (Aufhebung von Rechtsvorschriften)

32 (Änderung des Niedersächsischen Meldegesetzes)
33 (Änderung des Niedersächsischen Verfassungsschutzgesetzes) und
34 (In-Kraft-Treten)
wird abgesehen.

Erster Abschnitt

Allgemeine Bestimmungen

§ 1
Aufgabe des Gesetzes

[1)]Aufgabe dieses Gesetzes ist es, das Recht einer jeden Person zu gewährleisten, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). [2)]Dieses Gesetz bestimmt, unter welchen Voraussetzungen personenbezogene Daten durch öffentliche Stellen verarbeitet werden dürfen.

Zu § 1

Die Vorschrift greift auf den Wortlaut des **Volkszählungsurteils** des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65,1) zurück, um die Aufgabe des Gesetzes zu beschreiben. Anders als noch im NDSG 1978 beschränkt sich diese nicht mehr darauf, nur einen Missbrauch bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen zu verhindern. Satz 1 betont vielmehr entsprechend dem gewandelten Rechtsverständnis den umfassenden Schutzcharakter des Gesetzes für die Menschen und rückt ihn an die erste Stelle. Da im überwiegenden Allgemeininteresse Eingriffe in das **Grundrecht auf informationelle Selbstbestimmung** allerdings weiterhin möglich sein müssen, macht Satz 2 deutlich, dass das Gesetz zugleich ein Eingriffsgesetz darstellt, indem es bestimmt, unter welchen Voraussetzungen personenbezogene Daten durch öffentliche Stellen verarbeitet werden dürfen.

Eine informationelle Selbstbestimmung ist nur bei lebenden Personen möglich. Personenbezogene Daten Verstorbener fallen deshalb nicht in den Schutzbereich des NDSG. Für den Umgang mit diesen Daten ist die Rechtsprechung zum postmortalen Persönlichkeitsschutz heranzuziehen.

§ 2
Anwendungsbereich

(1) [1]Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen

1. **des Landes,**
2. **der Gemeinden und Landkreise,**
3. **der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts**

und deren Vereinigungen. [2]Sind einer Person oder Stelle außerhalb des öffentlichen Bereichs Aufgaben der öffentlichen Verwaltung übertragen, so ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(2) Der Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten und dabei die vom Landtag erlassene Datenschutzordnung anzuwenden haben.

(3) [1]Abweichend von Absatz 1 gelten nur die §§ 8, 19 und 26 sowie die Regelungen des Vierten Abschnitts, soweit personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeitet werden von

1. **juristischen Personen des öffentlichen Rechts oder deren organisatorisch selbständigen Einrichtungen, die am Wettbewerb teilnehmen,**
2. **wirtschaftlichen Unternehmen der Gemeinden und Landkreise ohne eigene Rechtspersönlichkeit (Eigenbetriebe) und Zweckverbänden, die überwiegend wirtschaftliche Aufgaben wahrnehmen,**
3. **öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden.**

[2]Für diese finden im Übrigen die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes in der Fassung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814), Anwendung.

(4) Auf öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen finden § 24 des Niedersächsischen Datenschutzgesetzes und im Übrigen die Vorschriften des Bundesdatenschutzgesetzes über nicht öffentliche Stellen Anwendung.

(5) Für öffentlich-rechtliche Rundfunkanstalten gilt das Recht des jeweiligen Sitzlandes.

(6) Besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten gehen den Bestimmungen dieses Gesetzes vor.

(7) Die Vorschriften dieses Gesetzes gehen denen des Niedersächsischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

(8) Auf das Gnadenverfahren findet dieses Gesetz mit Ausnahme des Vierten Abschnitts keine Anwendung.

Zu Abs. 1 und 2

1. Das Gesetz gilt für die Datenverarbeitung von Behörden und sonstigen öffentlichen Stellen Niedersachsens und deren Vereinigungen ohne Rücksicht auf den rechtlichen Charakter ihrer Tätigkeit. Auch das privatrechtliche Handeln der genannten Stellen wird damit erfasst. Ob eine Einrichtung eines Trägers öffentlicher Verwaltung als Behörde, als sonstige öffentliche Stelle oder als deren Vereinigung einzustufen ist, hängt maßgeblich vom Inhalt des Organisationsaktes ab, mit dem die Einrichtung gegründet wurde.

2. Das NDSG geht vom organisatorischen Behördenbegriff des Verwaltungsverfahrensrechts (§ 1 Abs. 4 NVwVfG) aus. **Behörde** ist danach jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

3. Der Geltungsbereich des Gesetzes erstreckt sich auch auf alle **sonstigen öffentlichen Stellen**. Nicht alle Stellen haben Behördencharakter (dieser fehlt z. B. bei den Einrichtungen, die anderen Behörden zuarbeiten oder für sie Sachleistungen erbringen), nehmen aber trotzdem Aufgaben der öffentlichen Verwaltung wahr, wie z. B. Landesbetriebe, Notare oder Gerichtsvollzieher. Auch Beliehene (s. Nr. 5) fallen unter den in Satz 1 genannten Begriff der öffentlichen Stelle.

Die öffentliche Stelle ist damit der gesetzliche Oberbegriff. Seine Verwendung stellt sicher, dass für den öffentlichen Bereich bei der Anwendung des Gesetzes keine Lücken bleiben.

3.1. Von dieser Grundkonzeption her unterliegt auch der **Landtag** als Legislativorgan den Vorschriften des NDSG. Da dessen Regelungen auf die Besonderheiten parlamentarischer Arbeit jedoch nicht zugeschnitten sind, hat der Gesetzgeber im Änderungsgesetz vom 21. Juni 2001 vorgesehen, den parlamentarischen Bereich von der Geltung des Gesetzes auszunehmen, sobald die Datenverarbeitung des Parlaments in einer vom Landtag zu erlassenden **Datenschutzordnung** bereichsspezifisch geregelt ist. Diese Regelung ist mit der Datenschutzordnung vom 14. November 2001 (Nds. GVBl. S. 726) getroffen worden. Die Einhaltung der Vorschriften der Datenschutzordnung überwacht eine Datenschutzkommission, die für die Dauer jeder

Wahlperiode aus Mitgliedern der im Landtag vertretenen Fraktionen gebildet wird. Wer glaubt, durch die Datenverarbeitung des Parlaments in seinen Rechten verletzt worden zu sein, kann zur Prüfung der von ihm beanstandeten Vorgehensweise die Datenschutzkommission anrufen. Die oder der Landesbeauftragte für den Datenschutz hat insoweit keine Kontrollbefugnis (s. § 22 Abs. 1 Satz 2).

3.2 Öffentliche Stellen sind auch die **Gerichte**. Zwar darf im Hinblick auf die richterliche Unabhängigkeit (Art. 97 GG) eine Kontrolle der richterlichen Tätigkeit durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz nicht stattfinden, die materiell-rechtlichen Anforderungen des Datenschutzrechts insbesondere zur Datensicherung (§ 7) haben jedoch auch die Gerichte zu erfüllen. Soweit sie in Verwaltungsangelegenheiten tätig werden, unterliegen auch sie der Kontrolle durch die oder den Landesbeauftragten für den Datenschutz.

3.3 Eine vergleichbare Situation besteht für den **Landesrechnungshof**. Auch für ihn gilt das NDSG. Die Kontrollbefugnisse der oder des Landesbeauftragten für den Datenschutz sind jedoch ebenfalls eingeschränkt (vgl. dazu insgesamt § 22 Abs. 1 Satz 2).

4. Das NDSG gilt grundsätzlich auch für **Vereinigungen,** die das Land, die Gemeinden und Landkreise sowie die sonstigen der unter Abs. 1 Nr. 3 genannten juristischen Personen des öffentlichen Rechts untereinander gebildet haben - auch wenn diese privatrechtlich organisiert sind. Eine Ausgliederung öffentlicher Aufgaben auf einen privatrechtlichen Träger, der diese Aufgaben in privatrechtlicher Form wahrnimmt, soll nicht zu einer Verschlechterung des Datenschutzes für die davon betroffenen Bürgerinnen und Bürger führen.

4.1 Bei der Vereinigung muss es sich, wie mit dem Gesetzeswortlaut „deren“ zum Ausdruck gebracht wird, um eine solche handeln, die von mehreren der unter Abs. 1 Nrn. 1, 2 und 3 genannten öffentlich-rechtlichen Trägern untereinander gebildet wurde (z. B. eine Vereinigung zwischen dem Land und den Kommunen). Die Sonderregelungen für so genannte „Wettbewerbsunternehmen“ (vgl. Abs. 3) sind zu beachten.

4.2 Vereinigungen, die nur von einem Rechtsträger gebildet werden (z. B. eine GmbH, bei der das Land über 100 Prozent der Anteile verfügt, oder die Bildung einer allein von einer Stadt gegründeten Gesellschaft mit beschränkter Haftung) werden vom Anwendungsbereich dieses Gesetzes nicht erfasst. Für diese Vereinigungen gelten die Vorschriften des BDSG.

4.3 Das NDSG schließt die Beteiligung nicht öffentlicher Stellen aus. Für Vereinigungen, an denen neben öffentlichen Stellen auch nicht öffentliche Stellen (natürliche Personen oder juristische Personen des privaten Rechts) beteiligt sind, gilt daher immer das BDSG.

5. Mit den in Abs. 1 Satz 2 genannten Personen oder Stellen außerhalb des öffentlichen Bereichs, denen Aufgaben der öffentlichen Verwaltung übertragen sind, sind ausschließlich **Beliehene** angesprochen. Ihnen sind durch gesetzlichen oder auf gesetzlicher Grundlage beruhenden Beleihungsakt staatliche Aufgaben übertragen worden (z. B. Kfz-Sachverständige des TÜV, öffentlich bestellte Vermessungsingeni-

eure, Feld- und Forsthüter). Private Auftragnehmer, die Daten im Auftrag einer öffentlichen Stelle und nach deren Weisung verarbeiten (§ 6), fallen nicht unter die Vorschrift.

Zu Abs. 3

5. Die in der Vorschrift genannten **Unternehmen**, die zusammenfassend als öffentliche Wettbewerbsunternehmen bezeichnet werden können, werden von der Geltung des NDSG weitgehend ausgenommen. Da sie sich in einer Wettbewerbssituation mit privaten Unternehmen befinden und durch die gegenüber den Datenschutzvorschriften im privaten Bereich strengeren Regelungen des NDSG keine Wettbewerbsnachteile erleiden sollen, gelten auch für diese öffentlichen Unternehmen grundsätzlich die materiellen Regelungen des BDSG. Nur den Vorschriften des NDSG zur Datenschutzkontrolle (§§ 19, 21 bis 23) sowie zur Verfahrensbeschreibung (§ 8) und zum Fernmessen und Fernwirken (§ 26) bleiben sie unterworfen.

Da die Regelung allein die Chancengleichheit im Wettbewerb sichern soll, gilt für die Datenverarbeitung, die nicht von der Wettbewerbssituation geprägt ist, wie z. B. die Verarbeitung von Beschäftigtendaten, weiterhin das NDSG, dem allerdings bereichsspezifische Regelungen (z. B. des NBG) vorgehen.

Die Ausübung **wirtschaftlicher Tätigkeit** muss im Übrigen für das Unternehmen bestimmend sein. Fiskalische Hilfsgeschäfte als bloße Begleiterscheinung der sonstigen Verwaltungstätigkeit (wie z. B. die Veräußerung ausgesonderter Dienst-Kfz) fallen nicht unter die Vorschrift.

6. Auf die Informationen auf meiner Homepage (www.lfd.niedersachsen.de) zum Thema „öffentlich-rechtliche Wettbewerbsunternehmen“ wird verwiesen.

Zu Abs. 4

7. § 24 NDSG findet als **bereichsspezifische Regelung** für die Datenverarbeitung personenbezogener Daten **bei Dienst- und Arbeitsverhältnissen der öffentlich-rechtlichen Kreditinstitute, der öffentlich-rechtlichen Versicherungsanstalten** sowie deren Vereinigungen Anwendung. Zu den öffentlich-rechtlichen Kreditinstituten zählen die Norddeutsche Landesbank, die Sparkassen und die Ritterschaftlichen Kreditinstitute; zu den öffentlich-rechtlichen Versicherungsanstalten gehören die öffentlichen Lebensversicherungsanstalten, die öffentliche Sachversicherung Braunschweig und die öffentlichen Brandversicherungsanstalten.

8. Im Rahmen der Ausübung ihrer wirtschaftlichen Tätigkeit unterfallen diese Stellen aus Gründen der Wettbewerbsgleichheit den für die privatrechtlichen Konkurrenzunternehmen geltenden Vorschriften des BDSG zur Datenverarbeitung bei nicht öffentlichen Stellen. Dies gilt jedoch nur, soweit personenbezogene Daten verarbeitet werden (s. Begründung zu § 2 Abs. 3 NDSG, LT-Drs. 12/3290).

Zu Abs. 6

9. In der Klarstellung, dass **bereichsspezifische Regelungen** zum Datenschutz den allgemeinen Vorschriften des NDSG vorgehen, wird zugleich der Querschnittscharak-

ter dieses Gesetzes deutlich. Das NDSG legt einen einheitlichen Datenschutzstandard für alle Tätigkeiten öffentlicher Stellen fest, deren Aufgabenerledigung nicht durch datenschutzrechtlich relevante Besonderheiten geprägt wird. Soweit besondere Anforderungen an die Verwaltungstätigkeit in einzelnen Verwaltungsbereichen eine weitergehende Einschränkung des Rechts auf informationelle Selbstbestimmung erforderlich machen, müssen entsprechende bereichsspezifische Datenschutzbestimmungen geschaffen werden. Als bereichsspezifische Vorschriften sind auch die im Fünften Abschnitt des Gesetzes enthaltenen Bestimmungen anzusehen, da sie von den allgemeinen Rechtsvorschriften zur Datenverarbeitung (§§ 9 bis 15) abweichen.

Verdrängt wird das NDSG durch Spezialvorschriften nur so weit, wie der Regelungsgehalt dieser speziellen datenschutzrechtlichen Vorschriften reicht (s. z. B. § 12 Abs. 2 BDSG).

Sind diese unvollständig, bleibt für die nicht geregelten Datenverarbeitungsvorgänge das NDSG anwendbar (s. § 88 Abs. 1 S. 2, 1. HS NBG). So werden z. B. die Vorschriften des NKomVG mit datenschutzrechtlichem Bezug durch das NDSG ergänzt.

Ein Rückgriff auf das NDSG ist allerdings dann ausgeschlossen, wenn die spezialgesetzlichen Regelungen als abschließend anzusehen sind (s. „soweit“-Regelung des § 88 Abs. 1 S. 2, 2. HS NBG).

Bei spezialgesetzlichen Vorschriften des Bundesrechts ist in diesem Zusammenhang die Gesetzgebungszuständigkeit zu beachten. Stellt sich heraus, dass eine Regelung unvollständig ist, für die der Bund die ausschließliche Gesetzgebungskompetenz besitzt, kann das NDSG nicht zur Lückenfüllung herangezogen werden. Das Gleiche gilt für eine Bundesregelung im Bereich der konkurrierenden Gesetzgebungszuständigkeit, die der Bund als abschließend versteht. Auch hier scheidet ein ergänzender Rückgriff auf das NDSG aus.

Die Verarbeitung der in § 4 Abs. 2 Satz 2 genannten besonders sensiblen Daten ist grundsätzlich nur auf der Grundlage bereichsspezifischer Vorschriften zulässig (s. a. § 10 Abs. 2 Satz 2).

Zu Abs. 7

8. Soweit es um die Ermittlung des Sachverhalts geht, verdrängt das NDSG die Vorschriften des über § 1 Abs. 4 NVwVfG geltenden VwVfG. Nach § 26 VwVfG bedient sich die Behörde der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann dazu Auskünfte jeder Art einholen und sich der unterschiedlichsten Quellen bedienen. Gemäß § 24 Abs. 1 Satz 2 VwVfG bestimmt die Behörde Art und Umfang ihrer Ermittlungen. Diese Regelungen sind mit datenschutzrechtlichen Grundsätzen (z. B. dem Vorrang der Datenerhebung beim Betroffenen, der Zweckbindung personenbezogener Daten) nicht vereinbar. Sie treten deshalb gegenüber den Bestimmungen des NDSG (§§ 9 ff.) zurück.

Eingeschränkt wird damit auch eine Datenübermittlung im Rahmen der **Amtshilfe**. Da die Amtshilfevorschriften den datenschutzrechtlichen Grundsatz der Zweckbindung

nicht berücksichtigen, darf Amtshilfe nur im Rahmen der einschränkenden Regelungen des NDSG (§ 11 Abs. 1 i. V. m. § 10 Abs. 2) geleistet werden. Zu einer weitergehenden Übermittlung ist die ersuchte Behörde nach § 5 Abs. 2 Nr. 1 VwVfG aus rechtlichen Gründen nicht in der Lage.

Das in § 29 VwVfG geregelte Recht auf Akteneinsicht der Verfahrensbeteiligten besteht dagegen neben dem Recht auf Auskunft und Akteneinsicht nach § 16 NDSG.

Dem NDSG vorgehende Regelungen enthalten die Bestimmungen des VwVfG über Planfeststellungsverfahren, soweit diese die Verarbeitung personenbezogener Daten zwingend voraussetzen. Dies ist z. B. bei der in § 74 Abs. 4 VwVfG vorgeschriebenen Zustellung und öffentlichen Auslegung des Planfeststellungsbeschlusses der Fall. Aus dem Verhältnismäßigkeitsgrundsatz ergeben sich allerdings im Einzelfall Einschränkungen für die Zulässigkeit der damit verbundenen Datenübermittlung. Inwieweit eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses es erfordert, dass die inhaltliche Auseinandersetzung mit den geltend gemachten Einwendungen personenbezogen vorgenommen und mit der Begründung veröffentlicht wird, ist deshalb im Einzelfall auch unter Berücksichtigung verwaltungspraktischer Gesichtspunkte zu prüfen.

Zu Abs. 8

9. Die Herausnahme des **Gnadenverfahrens** aus dem Anwendungsbereich des Gesetzes ist unbefriedigend, weil den Bediensteten, die bei dieser Verwaltungsaufgabe eingesetzt werden, datenschutzrechtliche Vorschriften für ihre Arbeit vorenthalten werden. Diese Mitarbeiterinnen und Mitarbeiter müssen sich deshalb unmittelbar an den Aussagen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung orientieren. Der Rechtsicherheit ist dies nicht förderlich. Dieser Mangel kann auch nicht dadurch ausgeglichen werden, dass der oder dem Landesbeauftragten für den Datenschutz eine Kontrollbefugnis in diesem Bereich eingeräumt worden ist.

§ 3
Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (Betroffene).

(2) [1]Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten. [2]Im Einzelnen ist

1. **Erheben das Beschaffen von Daten über die Betroffenen,**
2. **Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,**
3. **Verändern das inhaltliche Umgestalten von Daten,**
4. **Übermitteln das Bekanntgeben von Daten an Dritte in der Weise, dass**
   a) die Daten durch die Daten verarbeitende Stelle weitergegeben werden oder
   b) Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsehen oder abrufen,
5. **Sperren das Kennzeichnen von Daten, um ihre weitere Verarbeitung einzuschränken,**
6. **Löschen das Unkenntlichmachen von Daten,**
7. **Nutzen jede sonstige Verwendung von Daten.**

(3) Daten verarbeitende Stelle ist jede Stelle, die personenbezogene Daten selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt.

(4) [1]Empfänger ist jede Person oder Stelle, die Daten erhält. [2]Dritte sind Personen oder Stellen außerhalb der Daten verarbeitenden Stelle. [3]Dritte sind nicht die Betroffenen sowie diejenigen Personen und Stellen, die im Auftrag personenbezogene Daten verarbeiten (Auftragnehmer).

(5) Automatisierte Verarbeitung ist die Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

(6) [1]Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage und die Zusammenfassung solcher Unterlagen einschließlich der Bild- und Tonträger. [2]Hierunter fallen nicht Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

Zu Abs. 1

1. § 3 definiert die wesentlichen Begriffe des NDSG. Abs. 1 bestimmt einen Kernbegriff des Datenschutzrechts, den der **personenbezogenen Daten**. Hierunter werden

Einzelangaben über persönliche und sachliche Verhältnisse von bestimmten oder bestimmbaren Personen verstanden. Damit sind alle Angaben gemeint, die über eine lebende natürliche Person etwas aussagen, unabhängig davon, in welcher Form dies geschieht.

Den **persönlichen Verhältnissen** können z. B. Angaben wie Name, Geburtstag, Alter, Staatsangehörigkeit, Interessen, Weltanschauung, Familienstand, gesundheitliche Angaben, Werturteile über eine Person zugerechnet werden. Unter **sachlichen Verhältnissen** einer Person sind z. B. Angaben über Grundbesitz, über Abgaben, Steuern, Versicherungen oder Bankguthaben zu verstehen. Eine eindeutige Abgrenzung der Daten über persönliche Verhältnisse von denen über sachliche Verhältnisse ist wegen vielfacher Überschneidungen nicht möglich. Sie ist auch nicht erforderlich, da sich an diese Zuordnung keine unterschiedlichen Rechtsfolgen knüpfen. Im Einzelfall kann deshalb dahingestellt bleiben, ob eine Angabe sich auf sachliche oder auf persönliche Verhältnisse bezieht.

Einer **bestimmten Person** sind die Angaben zuzuordnen, wenn die betreffende Information auf eine konkrete Person verweist (wie z. B. Angaben in einem Ausweis); bestimmbar ist die Person hingegen, wenn der Personenbezug mit Hilfe von Zusatzwissen von der Daten verarbeitenden Stelle hergestellt werden kann. Beispiel: Ein Kfz-Kennzeichen lässt zwar noch keinen unmittelbaren Schluss auf eine bestimmte Person zu, diese ist jedoch bestimmbar, weil der Personenbezug mit Hilfe von Informationen über die Kfz-Zulassung hergestellt werden kann.

Einzelangaben liegen nicht vor, wenn Daten über mehrere Personen zu Gruppenangaben (Sammelangaben) zusammengefasst sind. Lassen die Gruppenangaben keinen Schluss auf eine Einzelperson mehr zu, ist das NDSG nicht anwendbar.

Die Vorschrift erfasst nur lebende natürliche Personen. Daten **Verstorbener** fallen nicht in den Schutzbereich des NDSG (s. Erläuterung zu § 1). Juristische Personen und nicht rechtsfähige Personengemeinschaften (z. B. nicht rechtsfähige Vereine, Wohngemeinschaften) haben ebenfalls kein Recht auf informationelle Selbstbestimmung. Enthalten Angaben über juristische Personen und Personengemeinschaften jedoch zugleich Informationen über eine natürliche Person, fallen diese Daten in den Schutzbereich des Gesetzes. Beispiel: Aus dem Namen einer Einzelfirma oder beim einzigen Gesellschafter einer Einmann-GmbH kann auf die hinter der Gesellschaft stehende Person geschlossen werden.

Zu Abs. 2

2. Abs. 2 definiert die Begriffe für die sieben **Phasen der Datenverarbeitung**. **Das NDSG geht** - anders als das BDSG - **von einem umfassenden Begriff der Datenverarbeitung aus**. § 3 Abs. 2 umfasst daher auch jede aktenmäßige Verarbeitung.

Erheben im Sinne dieser Vorschrift ist das zielgerichtete Beschaffen von Daten. Die Datenerhebung hat grundsätzlich beim Betroffenen zu erfolgen.

Speichern ist das Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem beliebigen Medium, dem Datenträger. Erfassen ist dabei das Fixieren der Daten auf dem Datenträger. Aufnehmen ist das Fixieren mit Hilfe von

Aufnahmetechniken, hierzu zählen u. a. Ton- und Bildaufzeichnungsgeräte wie Tonbandgeräte, Videorecorder oder elektronische Aufzeichnungsgeräte.

Verändern ist die inhaltliche Umgestaltung der gespeicherten Daten. Die Veränderung kann sich aus einer Verknüpfung von Daten aus verschiedenen Dateien, Übernahme von Daten in andere Vorgänge, der Veränderung der Reihenfolge oder des Zusammenhangs ergeben.

Übermitteln setzt voraus, dass die Daten an Dritte weitergegeben werden bzw. der Dritte die Daten tatsächlich einsieht oder abruft. Allein das Vorhalten von Daten zum Abruf stellt noch keine Übermittlung dar.

Sperren ist das vollständige oder teilweise Einschränken der weiteren Verwendung von personenbezogenen Daten durch eine besondere Kennzeichnung.

Löschen ist das Unkenntlichmachen von auf einem Datenträger fixierten personenbezogenen Daten. Dies kann von dem Überschreiben bzw. Überlagern einer Aufnahme durch eine neue Aufnahme, vom Schwärzen bis hin zur teilweisen oder vollständigen Vernichtung des Datenträgers geschehen.

Nutzen ist jede sonstige Verwendung von personenbezogenen Daten. Das Nutzen von Daten ist ein Auffangtatbestand, der immer dann greift, wenn eine Verwendung der Daten keiner anderen Phase der Datenverarbeitung zugeordnet werden kann. Damit wird sichergestellt, dass jede Datenverarbeitung vom Gesetz erfasst wird. Ein Nutzen liegt z. B. vor, wenn personenbezogene Daten mit einer bestimmen Zweckbindung ausgewertet und zusammengestellt werden. Ein Band- oder Dateiabgleich, der weder eine Speicherung noch eine Veränderung von Daten darstellt, ist ebenfalls ein Nutzen personenbezogener Daten. Auch die Weitergabe von Daten innerhalb einer Behörde im organisatorischen Sinne ist als Nutzen personenbezogener Daten anzusehen. Die Zulässigkeit der behördeninternen Datenweitergabe richtet sich nach § 11 Abs. 4.

Zu Abs. 3

3. **Daten verarbeitende Stelle** ist der Sammelbegriff für die in § 2 als Normadressaten des Gesetzes beschriebenen Personen und Stellen.

Die Daten verarbeitende Stelle bleibt auch bei der Beauftragung anderer Behörden und externer Dienstleister für die Einhaltung der datenschutzrechtlichen Bestimmungen während der von ihr veranlassten Verarbeitungen verantwortlich.

Zu Abs. 4

4. Der Begriff des **Empfängers** ist weit gefasst. Er umfasst neben dem Dritten, dem Betroffenen und denjenigen Personen und Stellen, die personenbezogene Daten verarbeiten, auch die verschiedenen Organisationseinheiten innerhalb einer speichernden Stelle.

Satz 3 erläutert den Begriff des **Dritten**. Danach ist Dritter jede natürliche bzw. juristische Person oder Stelle außerhalb der speichernden Stelle mit Ausnahme des Betroffenen und eines Auftragnehmers.

Zu Abs. 5

5. Das Änderungsgesetz vom 21. Juni 2001 verzichtet auf eine weitere Verwendung des **Dateibegriffs** im NDSG. Damit ist eine Begriffsbestimmung sowohl der automatisierten wie der nicht automatisierten Datei entfallen. Die frühere Dateibeschreibung wird ihrem geänderten Inhalt entsprechend jetzt als Verfahrensbeschreibung (§ 8) bezeichnet.

Für die Datenverarbeitung öffentlicher Stellen hat der **Dateibegriff** seine früher bestimmende Funktion eingebüßt. Während die Anwendbarkeit des NDSG 1978 noch eine dateimäßige Datenverarbeitung voraussetzte, hat bereits die Neufassung von 1993 das Gesetz auf **jede Art der Datenverarbeitung** erstreckt. Nur im nicht öffentlichen Bereich ist der Dateibegriff weiterhin von Bedeutung (vgl. die Definition in § 3 Abs. 2 Satz 2 BDSG).

An die Stelle des Begriffs der automatisierten Datei ist der Begriff der automatisierten Verarbeitung getreten. Seine Definition lehnt sich an das BDSG an. Beim Einsatz von Datenverarbeitungsanlagen erfolgen die einzelnen Verarbeitungsschritte nicht auf Grund menschlicher Entscheidungen in jeder Verfahrensphase, sondern auf Grund eines selbstständig ablaufenden Programms. Rechtsfolgen, die sich an die automatisierte Verarbeitung knüpfen, sind die Erstellung einer Verfahrensbeschreibung (§ 8), ggf. die Notwendigkeit einer Vorabkontrolle (§ 7 Abs. 3) und besondere technische und organisatorische Maßnahmen (§ 7).

Zu Abs. 6

6. **Akte** ist jede Unterlage, die von einer Stelle zu den genannten amtlichen oder dienstlichen Zwecken zum Nachweis eines Vorgangs geführt wird. **Unterlage** ist jeder Datenträger, auf dem Daten zu amtlichen und dienstlichen Zwecken fixiert werden; außer Schriftstücken sind auch Bild- und Tonträger Akten im Sinne dieser Vorschrift.

Nicht zur Akte gehören Vorentwürfe von Schriftstücken oder persönliche Notizen, die sich noch nicht auf den Betroffenen auswirken, sondern erst noch in den eigentlichen Vorgang aufgenommen werden sollen. Werden die Vorentwürfe zu Beweiszwecken aufgehoben, so werden sie Bestandteil der Akte.

§ 4
Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. **dieses Gesetz oder eine andere Rechtsvorschrift dies vorsieht oder**
2. **die Betroffenen eingewilligt haben.**

(2) [1]Die Einwilligung bedarf der Schriftform, es sei denn, dass wegen besonderer Umstände eine andere Form angemessen ist. [2]Soweit die Einwilligung personenbezogene Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben betrifft, muss sie sich ausdrücklich auf diese Angaben beziehen. [3]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. [4]Die Betroffenen sind in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung auch über die Empfänger der Daten aufzuklären. [5]Die Betroffenen sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern oder mit Wirkung für die Zukunft widerrufen können.

(3) Die Einwilligung ist unwirksam, wenn sie durch Androhung rechtswidriger Nachteile oder durch Fehlen der Aufklärung bewirkt wurde.

Zu Abs. 1

1. Als zentrale Regelung des Gesetzes legt die Vorschrift die grundlegenden Voraussetzungen für die **Verarbeitung personenbezogener Daten** fest. Eine Datenverarbeitung, die nicht auf eine **Rechtsvorschrift** des NDSG oder eines anderen Gesetzes oder auf eine **Einwilligung** gestützt werden kann, ist unzulässig. Zu den Rechtsvorschriften zählen neben Gesetzen und Rechtsverordnungen auch Satzungen, die von einer juristischen Person des öffentlichen Rechts im Rahmen der ihr verliehenen Autonomie erlassen werden, sowie allgemeinverbindliche tarifvertragliche Regelungen und Dienstvereinbarungen zwischen Dienststelle und Personalrat.

Zu Abs. 2

2. Fehlt eine einschlägige Rechtsvorschrift, darf die Datenverarbeitung nur mit Einwilligung, d.h. vorheriger Zustimmung des Betroffenen, erfolgen. Auf die Einwilligung kann jedoch nicht zurückgegriffen werden, wenn die gesetzlichen Voraussetzungen einer beabsichtigten Datenverarbeitung nicht erfüllt sind. Die Einwilligung kann die Handlungsmöglichkeiten öffentlicher Stellen über den gesetzlichen Rahmen hinaus nicht erweitern. Deshalb ist es z. B. nicht zulässig, sich mit Hilfe der Einwilligung für die Aufgabenerfüllung nicht erforderliche Daten zu verschaffen.

3. Die Einwilligung muss **hinreichend bestimmt** sein. Im Zeitpunkt der Abgabe der Erklärung müssen die Daten verarbeitende Stelle, die Art der zu verarbeitenden Daten, der Zweck der Verarbeitung, bei beabsichtigter Datenübermittlung auch die künftigen Datenempfänger eindeutig erkennbar sein. Für die in Satz 2 genannten besonders sensiblen Daten fordert das Gesetz zusätzlich, dass die Einwilligung sich ausdrücklich auf diese Daten bezieht. Diese Regelung geht auf Art. 8 der EG-Datenschutzrichtlinie zurück.

4. Über die Bedeutung der Einwilligung muss der Betroffene umfassend aufgeklärt werden. Er muss Inhalt und Tragweite seiner Erklärung überblicken können. Zur **Aufklärung** gehört auch ein Hinweis darauf, dass die Einwilligung verweigert oder mit Wirkung für die Zukunft widerrufen werden kann. Die jeweiligen Rechtsfolgen dieses Verhaltens sind darzustellen. Ein Widerruf für die Vergangenheit kommt nicht in Betracht, da Datenverarbeitungen, die auf Grund einer ursprünglich erteilten Einwilligung durchgeführt worden sind, nicht nachträglich die Rechtsgrundlage entzogen werden kann.

5. Wirksam ist die Einwilligung nur, wenn der Betroffene über die nötige Einsichtsfähigkeit verfügt, d. h. die Folgen einer Verarbeitung seiner Daten erkennen und sachgerecht einschätzen kann. Geschäftsfähigkeit ist dazu nicht erforderlich, da die Einwilligung nicht als Willenserklärung anzusehen ist.

Auch bei vorhandener Einsichtsfähigkeit einer/eines Minderjährigen (Beurteilung nach dem jeweiligen Reifezustand, im Regelfall ab der Vollendung des 15. Lebensjahres) ist neben der Einwilligung der/des Minderjährigen zusätzlich die Einwilligung der gesetzlichen Vertreter einzuholen.

6. Grundsätzlich bedarf die Einwilligung der **Schriftform**, d. h. sie muss vom Betroffenen eigenhändig unterzeichnet werden. Die Schriftform hat eine Warn- und eine Dokumentationsfunktion. Nur wenn wegen besonderer Umstände eine andere Form angemessen ist, kann von der Schriftform abgesehen werden. Sind solche Umstände nicht gegeben, ist die Einwilligung unwirksam (vgl. § 125 BGB). Im Einzelfall kann auch eine Einwilligung durch schlüssiges Verhalten (konkludente Einwilligung) in Betracht kommen. Zum Beispiel bringt ein Bewerber durch die Übersendung von einschlägigen Unterlagen zum Ausdruck, dass diese zur Bearbeitung des Bewerbungsvorganges gespeichert werden dürfen. Eine konkludente Einwilligung scheidet allerdings bei den in Satz 2 genannten besonders sensiblen Daten aus. Für diese ist zwar keine schriftliche, aber eine ausdrückliche Einwilligung erforderlich.

Eine Einwilligung, die im Zusammenhang mit anderen Erklärungen erteilt werden soll, ist im Schriftbild (z. B. durch Fett-, Kursivdruck oder Einrahmung) besonders hervorzuheben, damit der Betroffene auf Anhieb erkennen kann, dass ihm auch die Abgabe einer Einwilligung abverlangt wird.

Zu Abs. 3

7. Eine Verletzung der Aufklärungspflichten führt zur **Unwirksamkeit** der Einwilligung, etwa wenn die Aufklärung unterblieben ist. Unwirksam ist die Einwilligung auch, wenn dem Betroffenen Angaben vorenthalten werden, die eine sachgerechte Einschätzung

der Bedeutung der Einwilligung nicht ermöglichen (z. B. wenn keine Informationen über den Zweck der Datenverarbeitung gegeben werden). In solchen Fällen wird häufig schon die notwendige Bestimmtheit der Einwilligung fehlen.

§ 5
Datengeheimnis

Den Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, diese zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung ihrer Tätigkeit.

Zu § 5

1. Während die übrigen Vorschriften des Gesetzes die öffentlichen Stellen zu einem bestimmten Verhalten berechtigen oder verpflichten, richtet sich § 5 unmittelbar an die Personen, die dienstlich Zugang zu personenbezogenen Daten haben.

Ihnen ist es untersagt, Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren. Die Bedeutung der Zweckbindung (§ 10) wird damit besonders hervorgehoben. Nach ihrem Wortlaut erstreckt sich die Vorschrift dagegen nicht auf andere Formen unbefugter Datenverarbeitung.

Ein Verstoß gegen § 5 liegt z. B. bei einer Datenübermittlung von Personaldaten für Werbezwecke ohne Einwilligung des Betroffenen, etwa für einen Beitritt in eine Krankenversicherung bei Auszubildenden, vor. In einem solchen Fall der unbefugten Offenbarung kann man von einer Verletzung des Datengeheimnisses sprechen. Soweit der Regelungsgehalt der Vorschrift jedoch über solche Fallgestaltungen hinausgeht, ist die Überschrift missverständlich.

2. Der von der Vorschrift angesprochene Personenkreis ist weit zu fassen. Neben den **Beschäftigen öffentlicher Stellen** und ihrer **Auftragnehmer** (§ 6) fallen darunter alle Personen, die die dienstliche Möglichkeit haben, auf Daten faktisch zuzugreifen. Damit werden z. B. auch **kommunale Mandatsträger** erfasst. Ein Verstoß gegen § 5 liegt z. B. vor, wenn ein Bürgermeister von der Gemeinde Daten von Jungwählern erhält und diese an seine Partei weitergibt.

3. Eine Verletzung der Vorschrift stellt nach § 29 Abs. 1 Nr. 1 eine **Ordnungswidrigkeit** dar. Wird im Einzelfall eine unbefugte Datenverarbeitung gegen Entgelt, in Bereicherungs- oder Schädigungsabsicht vorgenommen, kommt nach § 28 eine Straftat in Betracht. Bei Bediensteten einer öffentlichen Stelle liegt in einem schuldhaften Rechtsverstoß zugleich ein Dienstvergehen bzw. eine Verletzung arbeitsvertraglicher Pflichten. Im Falle eines Schadenseintritts ist die Verletzung der Vorschrift für die Haftungsfrage von Bedeutung.

4. Auf die Informationen auf meiner Homepage (www.lfd.niedersachsen.de) zum Thema „Datengeheimnis“ und „Verpflichtungen“ wird verwiesen.

§ 6
Verarbeitung personenbezogener Daten im Auftrag

(1) [1]Werden personenbezogene Daten im Auftrag öffentlicher Stellen verarbeitet, so bleiben diese für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2]Die im Dritten Abschnitt genannten Rechte sind ihnen gegenüber geltend zu machen.

(2) [1]Die Auftragnehmer dürfen personenbezogene Daten nur im Rahmen der Weisungen der Auftraggeber verarbeiten. [2]Auftraggeber haben sich über die Beachtung der Maßnahmen nach § 7 und der erteilten Weisungen zu vergewissern.

(3) [1]Auftragnehmer müssen Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 7 bieten. [2]Aufträge, Weisungen zu technischen und organisatorischen Maßnahmen und die Zulassung von Unterauftragsverhältnissen sind schriftlich festzuhalten.

(4) [1]Sofern die Vorschriften dieses Gesetzes auf Auftragnehmer keine Anwendung finden, hat die Daten verarbeitende Stelle den Auftragnehmer zu verpflichten, jederzeit vom Auftraggeber veranlasste Kontrollen zu ermöglichen. [2]Wird der Auftrag außerhalb des Geltungsbereichs dieses Gesetzes durchgeführt, so unterrichtet der Auftraggeber die zuständige Datenschutzkontrollbehörde.

Zu Abs. 1

1. **Datenverarbeitung im Auftrag** ist dadurch gekennzeichnet, dass eine Daten verarbeitende öffentliche Stelle eine andere öffentliche oder private Stelle beauftragt, personenbezogene Daten für sie zu verarbeiten. Der **Auftraggeber** bleibt dabei weiterhin „Herr“ seiner Daten, der eingeschaltete **Auftragnehmer** betreibt für ihn gleichsam als „verlängerter Arm“ oder ausgelagerte Organisationseinheit die Datenverarbeitung in völliger Abhängigkeit von seinen Weisungen. Die Auftragsdatenverarbeitung kann sich auf einzelne Phasen der Datenverarbeitung, aber auch auf diese insgesamt erstrecken. Ihr Gegenstand sind Hilfstätigkeiten, insbesondere die technische Durchführung der Verarbeitung (z. B. die Einschaltung eines externen Rechenzentrums, sofern ausschließlich rechentechnische Vorgänge nach vorgegebenem Algorithmus ausgelagert werden, oder die Entsorgung von Datenträgern. Nicht hierunter fällt hingegen die Übertragung solcher Aufgaben oder Teilaufgaben, bei denen nicht alle vorzunehmenden Verarbeitungsschritte von vornherein festgelegt sind, z. B. wenn die Bearbeitung eines Antrages der Auslegung unbestimmter Rechtsbegriffe bedarf und eine algorithmische Lösung auf der Ebene der reinen technischen Abwicklung nicht gegeben ist). Einen eigenen Beurteilungs- oder Entscheidungsspielraum hat der Auftragnehmer nicht. Dies wäre mit seinem Abhängigkeitsverhältnis vom Auftraggeber nicht vereinbar. Die Einschaltung eines Sachverständigen, bei dem eine vollständige Weisungsgebundenheit nicht besteht, ist

deshalb nicht als **Auftragsdatenverarbeitung** anzusehen. Bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Verwaltungsaufgabe oder werden diese auf eine andere Stelle ganz oder nur teilweise übertragen, spricht man von **Funktionsübertragung**. Angesichts der verfassungsrechtlich geforderten Bindung der Verwaltung an Recht und Gesetz (Art. 20 Abs. 3 GG) kann eine funktionale Tätigkeit nur durch den Gesetz- und Verordnungsgeber (bzw. durch ein nach Landesrecht befugtes Organ oder das Vertretungsorgan einer juristischen Person des öffentlichen Rechts, z. B. einer Gemeinde oder einer Hochschule) zu einer Aufgabe gemacht werden, wobei damit gleichzeitig der Umfang der funktionalen Tätigkeit begrenzt und die zuständige Stelle bestimmt wird.

Soll die inhaltliche Wahrnehmung von Aufgaben in diesem Sinne vollständig oder in Teilbereichen auf andere Stellen übertragen werden, scheidet § 6 NDSG als rechtliche Grundlage hierfür aus. Da die Zuständigkeit für die Aufgabenerledigung durch Rechtsvorschrift in der Regel eindeutig definiert ist, kann die auf die bloße Datenverarbeitung als Hilfsfunktion zur Aufgabenerfüllung gerichtete Vorschrift des § 6 NDSG diese Festlegung nicht ändern. Voraussetzung ist vielmehr, dass eine solche Aufgabenverlagerung auf anderer rechtlicher Grundlage zulässig oder rechtlich möglich ist. Dies können u. a. gesetzliche Regelungen, Satzungen, Verwaltungsvereinbarungen oder vertragliche Regelungen sein, soweit diese ihrerseits die Grenzen beachten, die sich aus dem Grundgesetz, der Staatsorganisation oder anderen gesetzlichen Vorschriften ergeben. Dies ist keine datenschutzrechtliche Frage, die datenschutzrechtliche Norm des § 6 NDSG kann daher nicht Grundlage für staatsorganisationsrechtliche Entscheidungen sein.

2. Eine Datenweitergabe im Rahmen der Auftragsdatenverarbeitung stellt keine Datenübermittlung dar, da das Handeln des Auftragnehmers dem Auftraggeber zugerechnet wird. Hierfür bedarf es deshalb keiner Rechtsgrundlage. Sind die Grenzen der Auftragsdatenverarbeitung überschritten, richtet sich die Datenweitergabe dagegen nach den §§ 11 bis 15.

3. Rechtlich verantwortlich für das Handeln des Auftragnehmers bleibt der Auftraggeber. Er ist Daten verarbeitende Stelle im Sinne des Gesetzes (§ 3 Abs. 3). Allein gegen ihn richten sich die Rechte der Betroffenen nach § 16 ff.

4. Soweit **Wartungsarbeiten** durch andere Personen oder Stellen zwingend die Verarbeitung personenbezogener Daten erfordern, gilt ebenfalls § 6. Im Gesetzgebungsverfahren zum Änderungsgesetz vom 21. Juni 2001 hat der Gesetzgeber klargestellt, dass Aufgaben der Wartung und Fernwartung unter die Vorschrift fallen.

Zu Abs. 2 und 3

5. Der Auftraggeber hat im Falle der Auftragsdatenverarbeitung Folgendes zu beachten:

- Sorgfältige Auswahl der Auftragnehmer unter besonderer Berücksichtigung ihrer Eignung; dazu gehört auch, dass sie die Gewähr für die Einhaltung der notwendigen Datensicherungsmaßnahmen bieten.

- Schriftliche Erteilung der erforderlichen Weisungen zur Auftragserfüllung. Diese beziehen sich auf die Datenverarbeitung selbst und nicht etwa auf eine inhaltliche Aufgabenerledigung. Dazu gehören z. B. Weisungen zu technischen und organisatorischen Maßnahmen (§ 7), Regelung des Verfahrens zum Test und zur Freigabe der Programme, Verfahren zur Fortschreibung, Änderung, Löschung und Sperrung des Datenbestandes und die Zulassung von Unterauftragsverhältnissen.
- Kontrolle der Einhaltung von Weisungen an den Auftragnehmer.

Zu Abs. 4

6. Die Auftrag gebende Stelle hat Auftragnehmer, die dem NDSG nicht unterworfen sind (insbesondere private Auftragnehmer), vertraglich zu verpflichten, von ihr veranlasste Kontrollen zu ermöglichen.

Lässt eine öffentliche Stelle des Landes personenbezogene Daten im Auftrag von einer **Stelle außerhalb Niedersachsens** verarbeiten, so hat der Auftraggeber die zuständige Datenschutzkontrollbehörde zu unterrichten. Handelt es sich bei dem Auftragnehmer um eine öffentliche Stelle eines anderen Landes oder des Bundes, so ist zuständige Datenschutzkontrollbehörde die oder der Datenschutzbeauftragte des jeweiligen Landes bzw. die oder der Bundesbeauftragte für den Datenschutz. Handelt es sich bei dem Auftragnehmer um eine nicht öffentliche Stelle, ist die nach § 38 BDSG zuständige Aufsichtsbehörde zu unterrichten.

§ 6 a
Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Stellen, die personenbezogene Speicher- und Verarbeitungsmedien herausgeben oder die auf solchen Medien Verfahren zur automatisierten Verarbeitung personenbezogener Daten aufbringen oder ändern, müssen die betroffene Person in allgemein verständlicher Form

1. **über ihre Identität und Anschrift,**
2. **über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,**
3. **darüber, wie die betroffene Person ihre Rechte nach den §§ 16 und 17 ausüben kann, und**
4. **über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen**

unterrichten, soweit die oder der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichteten Stellen haben dafür Sorge zu tragen, dass die zur Wahrnehmung der Rechte nach den §§ 16 und 17 erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Die Tatsache der Kommunikation des mobilen personenbezogenen Speicher- und Verarbeitungsmediums muss für die betroffene Person eindeutig erkennbar sein.

Zu Abs. 1

1. Mit dem Begriff „**mobile personenbezogene Speicher- und Verarbeitungsmedien**“ werden nach dem heutigen Stand der Technik vor allem **Chipkarten** erfasst. Allerdings sind neuere Techniken in der Entwicklung und teilweise bereits verfügbar, die nicht in Form einer Karte und auch ohne Chip personenbezogene Daten speichern, selbst nutzen oder für Dritte lesbar machen. Gemeinsame Wesensmerkmale sind:

- Die Systeme werden von einer Stelle an die Betroffenen ausgegeben,
- es existieren Schnittstellen, die von den ausgebenden Stellen und von Dritten zum Datenaustausch benutzt werden können,
- durch den Datenaustausch können auf den mobilen Systemen selbst oder auf stationären Systemen Datenverarbeitungsvorgänge angestoßen werden.

2. Die Vorschrift erfasst nur solche Systeme, auf denen Daten der Personen verarbeitet werden, die die Systeme im Besitz haben; die Systeme müssen an sie ausgegeben worden sein. Nicht erfasst werden tragbare Computer (z. B. Laptop, Smartphone, Tablet-PC), die an Mitarbeiter zur mobilen Aufgabenerfüllung herausgegeben werden.

3. Mobile personenbezogene Speicher- und Verarbeitungsmedien sind für die Besitzer häufig undurchschaubar. Sie können regelmäßig nicht selbst feststellen, was in den Datenverarbeitungssystemen gespeichert, auf andere Systeme übertragen und genutzt wird.

Damit die fehlende Transparenz bei der Datenverarbeitung mit dem mobilen System keine Beeinträchtigung der Rechte der Betroffenen bewirkt, schreibt Abs. 1 eine **Unterrichtungspflicht** für die ausgebende Stelle und für alle Stellen, die auf solchen Medien Verfahren zur automatisierten Verarbeitung personenbezogener Daten aufbringen oder ändern, vor. Betroffene müssen in allgemein verständlicher Form

- über Identität und Anschrift der Stellen,
- über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden Daten,
- darüber, wie die betroffenen Personen ihre Rechte auf Auskunft, Berichtigung, Löschung und Sperrung ausüben können, und
- über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichtet werden.

Zu Abs. 2

4. Die Betroffenen müssen die Möglichkeiten haben, jederzeit feststellen zu können, welche Daten über sie auf dem Medium gespeichert sind. Abs. 2 verpflichtet die am Verfahren beteiligten Stellen, in angemessenem Umfang Geräte oder Einrichtungen zur Verfügung zu stellen, mit denen die Betroffenen die auf dem Medium gespeicherten Daten für sich sichtbar machen können. Betroffene sollen ihr Recht verwirklichen können, ohne unzumutbare Wege oder sonstige Erschwernisse in Kauf nehmen zu müssen.

Zu Abs. 3

5. Um zu verhindern, dass ein Datenaustausch stattfindet, bei dem die betroffene Person nichts bemerkt (z. B. bei berührungslosen Chipkarten), verpflichtet Abs. 3 die beteiligten Stellen, die Tatsache der Kommunikation für die betroffene Person eindeutig erkennbar zu machen (z. B. durch akustische Signale).

§ 7
Technische und organisatorische Maßnahmen

(1) [1]Öffentliche Stellen haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung personenbezogener Daten sicherzustellen. [2]Der Aufwand für die Maßnahmen muss unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen.

(2) Werden personenbezogene Daten automatisiert verarbeitet, so sind Maßnahmen zu treffen, die je nach Art der Daten und ihrer Verwendung geeignet sind,

1. **Unbefugten den Zugang zu den Verarbeitungsanlagen zu verwehren (Zugangskontrolle),**
2. **zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),**
3. **die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),**
4. **zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),**
5. **zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),**
6. **zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit an wen übermittelt worden sind (Übermittlungskontrolle),**
7. **zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),**
8. **zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),**
9. **zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle),**
10. **zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),**

11. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) Ein automatisiertes Verfahren darf nur eingesetzt oder wesentlich geändert werden, soweit Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien entstehen können, durch Maßnahmen nach Absatz 1 wirksam beherrscht werden können. Die nach Satz 1 zu treffenden Feststellungen sind schriftlich festzuhalten.

(4) Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten.

(5) Personenbezogene Daten, die in Akten oder in anderer Weise ohne Einsatz automatisierter Verfahren verarbeitet werden, sind insbesondere vor dem Zugriff Unbefugter zu schützen.

Zu § 7

1. Das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verlangen neben dem rechtlichen Schutz der personenbezogenen Daten auch, dass eine angemessene **Datensicherheit** gewährleistet ist. Hierfür sind **Gestaltungsregeln** erforderlich, die dem **Stand der Technik** entsprechen. Ziel dieser Regeln sollte es sein, Datenschutz mit der Technik und damit „an der Quelle der Risiken“ zu erreichen. Die Technikentwicklung sollte sich an den Zielsetzungen des Datenschutzes orientieren.

2. Der geltende Rahmen des NDSG für den technischen und organisatorischen Datenschutz (die „elf Gebote“ in Form der **Kontrollziele des Abs. 2**) erfüllt dieses Ziel nur unzureichend. Die Bestimmungen des § 7 Abs. 2 stammen überwiegend aus den 70er Jahren, in denen Datenverarbeitung ausschließlich in zentralistisch organisierten Rechenzentren stattfand. Der Datenschutz war geprägt von der Vorstellung einer monolithischen Großrechnerwelt und primär verbunden mit dem Schutz der Rechner, die in hermetisch abgeschlossenen Rechenzentren betrieben wurden. Die rasante Entwicklung der Informations- und Kommunikationstechnik hat heute die schnelle Verarbeitung großer Datenmengen, eine weltweite Kommunikation in digitalen Netzen ohne Grenzen und Zeitverzug bis hin zur Cloud basierten Verarbeitung sowie die jederzeitige Erreichbarkeit an allen Plätzen der Welt - nicht nur von Arbeitsplätzen, sondern auch von mobilen Endgeräten wie Notebooks, Tablet-PCs oder Smartphones - möglich gemacht. Datensicherung ist heute nicht mehr an technischen Anlagen festzumachen, sondern – im eigentlichen Sinne des Wortes – an den Daten selbst.

Sechs elementare Schutzziele

Eine den heutigen und auch künftigen Anforderungen einer komplexen IT-Welt gerecht werdende Definition des Schutzbereiches im Sinne des Datenschutzes sollte die sechs folgenden Kernziele umfassen:

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte auf Verfahren und Daten zugreifen und zur Kenntnis nehmen können (**Vertraulichkeit**),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (**Integrität**),
3. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),
4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (**Transparenz**),
5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (**Nichtverkettbarkeit**) und
6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte (z. B. nach den §§ 16 ff) wirksam ermöglichen (**Intervenierbarkeit**).

Aus diesen elementaren Schutzzielen lassen sich weitere – aus Rechtsprechung und Kommentierung teils wohlbekannte - Anforderungen ableiten, die je nach Anwendungsszenario zur Beurteilung zusätzlicher Teilaspekte einer datenschutzgerechten Verfahrensgestaltung herangezogen werden können.

So ist im Einzelfall zu fordern, dass bei der automatisierten Verarbeitung personenbezogener Daten auch Maßnahmen zu treffen sind, die gewährleisten, dass u. a.

- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität,** Teil der Integrität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**; Teil der Transparenz).

Die Schutzziele dienen als umfassender Maßstab für die Zielbestimmung, die sich aus den Grundrechten und der Rechtsprechung des Bundesverfassungsgerichtes (Persönlichkeitsrechte, Recht auf informationelle Selbstbestimmung, Schutzanspruch auf Integrität und Vertraulichkeit informationstechnischer Systeme) ergibt. Sie sind insbesondere geeignet die Basis für eine systematisierte technisch-organisatorische Ausgestaltung oder Prüfung von informationstechnischen Systemen (Hard- und Software), von geplanten und implementierten IT-Verfahren sowie der damit einhergehenden Abläufe und Geschäftsprozesse zu bilden. In der Praxis bedeutet dies, dass sich auf dieser Grundlage der Schutzziele der erforderliche Katalog von konkreten Datenschutzmaßnahmen entwickeln lassen.

Diese modernen Schutzziele sind technologieunabhängig; sie stellen einen allgemein gültigen Sicherheitsrahmen dar, der auch bei neuen Formen der Datenverarbeitung Bestand haben wird. Das NDSG orientiert sich entgegen meinen Empfehlungen nicht an diesen Zielsetzungen, sondern hält an den „elf Geboten“ der Datensicherung fest. Die überfällige Überarbeitung der Technikregeln hin zu einem durchgreifenden Systemdatenschutz wurde in Niedersachsen leider wiederholt zurückgestellt; es wurde auf eine grundsätzliche Überarbeitung in einem späteren Gesetzgebungsverfahren verwiesen.

Zu Abs. 1

3. Zu Datensicherungsmaßnahmen sind alle öffentlichen Stellen verpflichtet. Hierzu gehören alle Stellen, die personenbezogene Daten selbst verarbeiten oder – als Auftraggeber – durch andere verarbeiten lassen. Zusätzlich sind auch diejenigen öffentlichen Stellen erfasst, die für andere Stellen – und damit als Auftragnehmer im Sinne des § 6 – Daten verarbeiten. Auftraggeber und Auftragnehmer haben nebeneinander für die Einhaltung der angemessenen technischen und organisatorischen Maßnahmen zu sorgen. Der Auftraggeber ist grundsätzlich für die Einhaltung der Datenschutzvorschriften verantwortlich. Er sollte alle erforderlichen Datensicherungsmaßnahmen konzipieren und festlegen. Die vom Auftragnehmer zu treffenden Maßnahmen sollten dann im Vertrag zur Erteilung des Auftrages verpflichtend geregelt werden. Der Auftragnehmer ist nur für die Gewährleistung der Datensicherung für die Phasen der Datenverarbeitung verantwortlich, die er tatsächlich abwickelt. Der Auftraggeber hat sich über die Beachtung der Maßnahmen nach § 7 und der erteilten Weisungen zu vergewissern (§ 6 Abs. 2 Satz 2).

4. Die erforderlichen technischen und organisatorischen Maßnahmen sind unabhängig davon zu treffen, ob personenbezogene Daten in Akten oder mit Einsatz automatisierter Verfahren verarbeitet werden. Erforderlich ist ein **Datensicherungskonzept** aus technischen und organisatorischen Maßnahmen, das in seiner Gesamtheit einen hinreichenden Schutz der Daten vor unsachgemäßer Handhabung gewährleistet. Unsachgemäße Handhabung umfasst hierbei nicht nur Missbrauch, sondern darüber hinaus auch unzureichenden Schutz vor menschlichen Fehlhandlungen, organisatorischen Mängeln, technischem Versagen und höherer Gewalt.

Für die Beurteilung der **Angemessenheit** von Datensicherheitsvorkehrungen ist die Summe aller Maßnahmen entscheidend. Dabei ist der finanzielle Aufwand mit zu berücksichtigen. Soweit im Einzelfall eine Anforderung durch eine bestimmte Maßnahme nicht voll erfüllt wird, ist die dadurch entstehende Lücke durch entsprechende andere Maßnahmen zu schließen.

Das Datensicherungskonzept ist regelmäßig zu überprüfen und dem **Stand der Technik** anzupassen. Als Stand der Technik sind Produkte und Verfahren anzusehen, die ausreichend erprobt und „marktgängig“ sind.

Zu Abs. 2

5. Die geltenden elf Kontrollmaßnahmen sind nicht als starre Vorgabe zu verstehen. Vielmehr ist jeweils eine Abwägung zwischen der Sensibilität und Bedeutung der Daten, den potentiellen Gefahren, dem Grad der Schutzbedürftigkeit und dem mit den Sicherungsmaßnahmen verbundenen Aufwand zu treffen. Werden sensible und weniger sensible Daten gemeinsam verarbeitet, bestimmt sich das Schutzniveau nach den Daten mit der höchsten Sensibilität.

Grundsätzlich sind technische Datensicherungsmaßnahmen gegenüber organisatorischen Maßnahmen vorzuziehen. Bei der Auswahl der technischen Maßnahmen sollten sicherheitsüberprüfte und zertifizierte Produkte bevorzugt werden. Einen aktuellen Nachweis über sicherheitsüberprüfte Produkte führt das Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 183, 53133 Bonn (Internet: www.bsi.bund.de).

Die IT-Grundschutzkataloge des BSI beschreiben mögliche Gefahren und bieten einen umfangreichen Katalog geeigneter Datensicherungsmaßnahmen. Reichen auf Grund eines höheren Schutzbedarfes Grundschutzmaßnahmen nicht aus, sind weitergehende Zusatzmaßnahmen zu treffen.

Die BSI-Standards 100-x bieten zudem umfassende Orientierung für die Organisation eines Informationssicherheitsprozesses (BSI-Standard 100-1: Managementsysteme für Informationssicherheit – ISMS, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz und BSI-Standard 100-4: Notfallmanagement).

Bei konkreten Fragen, welche Sicherungsmaßnahmen erforderlich und angemessen sind, berät die oder der Landesbeauftragte nach § 22 Abs. 1.

Zu Abs. 2 Nr. 1

6. Unbefugten soll der Zugang zu Verarbeitungsanlagen verwehrt werden. Zur Auswahl angemessener Kontrollmaßnahmen ist es erforderlich, alle Verarbeitungsanlagen zu erfassen und festzulegen, wer unter welchen Bedingungen Zugang zu den Anlagen erhalten darf.

Zu Abs. 2 Nr. 2

7. Um wirksam zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können, ist auch hier für die richtige Auswahl der Maßnahmen eine umfassende Bestandsaufnahme aller papiernen und elektronischen Datenbestände, in denen zulässigerweise personenbezogene Daten gespeichert sind, durchzuführen und festzulegen, welche Mitarbeiterinnen und Mitarbeiter in welchem Umfang Zugriff auf diese Datenbestände haben. Danach sind angemessene und hinreichende Datensicherungsmaßnahmen auszuwählen und einzuführen.

Zu Abs. 2 Nr. 3, 4 und 5

8. Die unbefugte Eingabe in ein Datenverarbeitungssystem sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten ist zu verhindern. Das gilt nicht nur für Fremde, sondern auch für Mitarbeiterinnen und Mitarbeiter der Daten verarbeitenden Stelle, soweit der Zugriff nicht **zur Aufgabenerfüllung erforderlich** ist. Bevor mit der Datenverarbeitung begonnen werden kann, müssen die Benutzerinnen und Benutzer ihre Berechtigung im Einzelfall nachgewiesen haben. Dies geschieht heute überwiegend durch die Eingabe einer Benutzerkennung (Login und Passwort). Zunehmend werden chipkartenbasierte oder biometrische Identifikationsverfahren eingesetzt. Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, sind zu protokollieren und zu kontrollieren.

Zu Abs. 2 Nr. 6

9. Werden personenbezogene Daten übermittelt, muss protokolliert werden, welche Daten zu welcher Zeit an wen übermittelt worden sind. Sensible personenbezogene Daten sind verschlüsselt zu übermitteln. Es ist sicherzustellen, dass der Empfänger über Verfahren und Geräte zum Entschlüsseln verfügt.

Zu Abs. 2 Nr. 7

10. Die Verantwortung für die einzelnen Datenverarbeitungsprozesse muss zweifelsfrei festgestellt werden können, dies gilt in besonderem Maße für die Eingabe von Daten. Die daraus resultierenden Sicherungsmaßnahmen können zwar unbefugte Aktivitäten nicht von vornherein abblocken, sie können aber bewirken, dass zweifelhafte Aktivitäten unterbleiben, weil der „Veranlasser“ damit rechnen muss, zur Rechenschaft gezogen zu werden.

Zu Abs. 2 Nr. 8

Mit der Verfügbarkeitskontrolle sollen personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Hierunter fallen z. B. alle Maßnahmen, die u. a. nach Systemabstürzen sowohl die Wiederinbetriebnahme von Datenverarbeitungssystemen als auch den sicheren Zugriff auf konsistente und vollständige Datenbestände gewährleisten.

Zu Abs. 2 Nr. 9

12. Die Auftragskontrolle obliegt primär dem Auftraggeber. Er hat sich über die Beachtung der Maßnahmen nach § 7 und der erteilten Weisungen zu vergewissern (§ 6 Abs. 2 Satz 2).

Zu Abs. 2 Nr. 10

13. Der Transport von Datenträgern ist so zu sichern, dass Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Durch Verschlüsselung der Daten kann dies weitgehend, wenn auch nicht vollständig gewährleistet werden. Es ist jedoch sicherzustellen, dass die Verfahren und Geräte, mit denen die verschlüsselten Daten lesbar gemacht werden können, verfügbar sind.

Zu Abs. 2 Nr. 11

14. Organisatorische Maßnahmen treten neben technische Datensicherungsmaßnahmen. Mit Ihnen lassen sich technische Sicherheitsdefizite kompensieren. Beispiele:

- Anweisungen zur Passwortgestaltung,
- Anweisungen zum Umgang mit dem Internet,
- Löschungsfristen für Textdokumente,
- Vernichtung von Altakten,
- Prüfung und Aufbewahrung von Benutzungsprotokollen,
- Überwachung von Administrations- und Wartungsarbeiten,
- Verfahrensentwicklung, Verfahrensdokumentation und Freigabe.

Eine Dienstanweisung zum datenschutzgerechten Einsatz der Informations- und Kommunikationstechnik sollte alle Festlegungen dokumentieren und damit für die Benutzerinnen und Benutzer transparent machen.

Zu Abs. 3

15. Zur Prüfung der Zulässigkeit einer automatisierten Verarbeitung sind Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken in sich tragen, vor ihrer Einführung einer **Vorabkontrolle** (früher: Technikfolgenabschätzung) zu unterziehen, um festzustellen, ob die mit der **automatisierten Verarbeitung** verbundenen Risiken für die Rechte der Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

Personenbezogene Daten, deren automatisierte Verarbeitung **besondere Risiken** für die Rechte der Betroffenen mit sich bringen, sind solche, deren Missbrauch Existenz, Leben oder Freiheit der Betroffenen gefährden oder sie in ihrer gesellschaftlichen Stellung erheblich beeinträchtigen würden (siehe hierzu auch das **Schutzstufenkonzept** unter www.lfd.niedersachsen.de).

Neue Technologien sind solche, die erstmals im Anwendungsbereich des NDSG zum Einsatz kommen und bei denen noch nicht abschätzbar ist, ob die mit der Verarbeitung verbundenen Risiken für die Rechte der Betroffenen mit Maßnahmen nach § 7 Abs. 2 beherrscht werden können.

Dem Einsatz von Videoüberwachung muss gemäß § 25a Abs. 6 stets eine Vorabkontrolle vorausgehen. Diesem Grundsatz folgend sind darüber hinaus auch bei allen anderen Videoüberwachungsmaßnahmen (auf spezialgesetzlicher Grundlage), ohne Rücksicht auf die angewandte Technik, Vorabkontrollen zu fertigen.

Die Vorabkontrolle hat zu erfolgen, **bevor ein neues Verfahren seinen Wirkbetrieb aufnimmt**. Die Stelle, die den Einsatz des Verfahrens plant, hat die erforderlichen Informationen zur Verfügung zu stellen.

Auch **vor wesentlichen Änderungen** an Verfahren, für die schon bei Einführung eine Vorabkontrolle durchgeführt worden ist, ist eine erneute Prüfung durchzuführen.

Eine wesentliche Änderung liegt z. B. vor, wenn ein Verfahren so verändert wird, dass bei den nach § 8 Satz 1 aufzunehmenden Angaben substantielle Änderungen auftreten.

Die Ergebnisse der Vorabkontrolle sind **schriftlich** zu dokumentieren. Dabei sind den denkbaren Gefährdungen die möglichen Sicherungs- und Vorbeugungsmaßnahmen gegenüberzustellen. Verbleibende Gefahren für die Rechte der Betroffenen sind darzustellen und zu bewerten. Verfahrensalternativen zur angestrebten Lösung sind aufzuzeigen.

Die Aufgabe der Vorabkontrolle obliegt den behördlichen Datenschutzbeauftragten. In Zweifelsfällen ist die oder der Landesbeauftragte für den Datenschutz zu beteiligen (§ 8 a Abs. 3 Satz 3).

Zu Abs. 4

16. Mit dem **Gebot der Datenvermeidung und Datensparsamkeit** wird der Grundsatz der Verhältnismäßigkeit für die technische Gestaltung der Datenverarbeitungssysteme und -programme im Sinne eines Systemdatenschutzes konkretisiert. Die Regelung ist vom Erforderlichkeitsprinzip abzugrenzen; die Erforderlichkeit als materiell-rechtliche Anforderung beschränkt nur den Umfang der Datenverarbeitung im Einzelfall.

Der Grundsatz der Datenvermeidung und Datensparsamkeit gebietet, schon im Vorfeld bei Entwicklung und Auswahl von Datenverarbeitungssystemen darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden müssen. Er gibt damit ein übergreifendes Gestaltungsprinzip vor, das aus dem Tele- und Medienrecht übernommen worden ist. Es soll das Entstehen von Daten mit Personenbezug oder Personenbeziehbarkeit von vornherein ausschließen oder auf ein Minimum beschränken. Dieses Prinzip ist Bestandteil eines neuen Ansatzes, der über einen Systemdatenschutz eine Reduzierung der Risiken für die informationelle Selbstbestimmung erreichen will. Besondere Bedeutung für die Erreichung dieser Ziele haben die **Anonymisierung** und die **Pseudonymisierung**.

Zu Abs. 5

17. Auch für die nicht automatisierte Verarbeitung gelten die Datensicherungsgrundsätze, insbesondere sind die Datenträger vor dem Zugriff Unbefugter zu schützen.

§ 8
Verfahrensbeschreibung

[1]Jede öffentliche Stelle, die Verfahren zur automatisierten Verarbeitung personenbezogener Daten einrichtet oder ändert, hat in einer Beschreibung festzulegen:

1. **die Bezeichnung der automatisierten Verarbeitung und ihre Zweckbestimmung,**
2. **die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,**
3. **den Kreis der Betroffenen,**
4. **die Art regelmäßig zu übermittelnder Daten, deren Empfänger, in den Fällen des § 6 auch die Auftragnehmer, sowie die Herkunft regelmäßig empfangener Daten,**
5. **die Absicht, Daten in Staaten nach § 14 zu übermitteln,**
6. **Fristen für die Sperrung und Löschung der Daten,**
7. **die technischen und organisatorischen Maßnahmen nach § 7,**
8. **die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.**

[2]Satz 1 gilt nicht, wenn die Daten nur vorübergehend und zu einem anderen Zweck als dem der inhaltlichen Auswertung gespeichert werden, sowie für Register nach § 8 a Abs. 4 und Verarbeitungen nach § 8 a Abs. 5 Satz 1.

Zu § 8 Satz 1

1. Daten verarbeitende Stellen (z. B. deren Fachbereiche oder IT-Servicestellen) haben grundsätzlich für jedes von ihnen betriebene Verfahren zur automatisierten Verarbeitung personenbezogener Daten eine sog. **Verfahrensbeschreibung** zu erstellen und aktuell zu halten. Um Transparenz und Auskunftsfähigkeit gegenüber Betroffenen sowie Revisionsfähigkeit zu erreichen, ist darin zu dokumentieren, welche personenbezogenen Daten mit Hilfe welcher automatisierter Verfahren auf welche Weise verarbeitet werden und welche Datenschutzmaßnahmen dabei getroffen wurden.

Die Verfahrensbeschreibung wird in aller Regel die Daten verarbeitende Stelle selbst erstellen. Denkbar wäre aber auch, dass sie die Beschreibung durch eine andere Stelle für sich anfertigen lässt (z. B. durch ein als Auftragnehmer eingeschaltetes Rechenzentrum).

Die Verfahrensbeschreibung ist dem behördlichen Datenschutzbeauftragten zwecks Aufnahme in das Verfahrensverzeichnis (vgl. § 8 a Abs. 2 S. 5 NDSG) zur Kenntnis zuzuleiten.

2. Mit der Verwendung des Begriffs „Verfahren zur automatisierten Verarbeitung“ wird deutlich gemacht, dass die Verpflichtung zur Erstellung einer Verfahrensbeschreibung nicht an die einzelnen Verarbeitungsvorgänge anknüpft, vielmehr wird damit die Gesamtheit aller automatisierten Verarbeitungsschritte für einen bestimmten Verwaltungszweck (z. B. automatisierte Zeiterfassung) angesprochen.

3. Eine Verfahrensbeschreibung ist z. B. zu erstellen für

- Datenbankanwendungen,
- Dokumentensammlungen, die nach Autoren, Dokumententypen mit gleicher Sensibilität und Inhalten zusammengefasst sind (u. a. Bewilligungsbescheide, Bußgeldbescheide, Gutachten des Ärztlichen Dienstes) und
- Adressentabellen,
- Videoüberwachungsanlagen.

Zu § 8 Satz 2

4. Der Erstellung einer Verfahrensbeschreibung bedarf es nicht bei

- personenbezogenen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert und genutzt werden;
- Verfahren automatisierter Verarbeitung personenbezogener Daten, die nur vorübergehend und zu einem anderen Zweck als dem der inhaltlichen Auswertung gespeichert werden. Als vorübergehend ist dabei eine Speicherung anzusehen, wenn die Daten innerhalb von 3 Monaten nach ihrer Erstellung gelöscht werden;
- Registern, die zur Information der Öffentlichkeit bestimmt sind und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse geltend machen, zur Einsichtnahme offen stehen (z. B. Liegenschaftskataster, vgl. Erläuterungen zu § 8 a Abs. 4 NDSG);
- Verarbeitungen, von denen keine Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung zu erwarten sind (vgl. Erläuterungen zu § 8 a Abs. 5 Satz 1 NDSG sowie § 2 der als Anlage beigefügten Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten vom 10. Juli 2002, Nds. GVBl. S. 349).

Auch wenn keine Dokumentationspflicht besteht, muss die zuständige Stelle Datenschutzvorkehrungen nach § 7 NDSG treffen. Bei der Textverarbeitung ist z. B. zu regeln, wann welche Texte mit personenbezogenem Inhalt zu löschen sind.

5. Problematisch sind in der Praxis immer wieder Dateien, die mit Hilfe von Bürokommunikationsprogrammen (wie z. B. Textverarbeitungs- oder Tabellenkalkulationsprogrammen) erstellt worden sind.

Kennzeichnend für ein automatisiertes Verfahren ist die Verarbeitung personenbezogener Daten für einen bestimmten Zweck. Ein Bürokommunikationsprogramm, für sich allein betrachtet, kann daher kein automatisiertes Verfahren sein, weil kein Bezug zur Verarbeitung personenbezogener Daten besteht. Im Gegensatz dazu sind

Bürokommunikationsprogramme und eine oder mehrere damit erstellte Dateien, mit denen personenbezogene Daten für einen bestimmten Zweck verarbeitet werden, automatisierte Verfahren.

Um ein automatisiertes Verfahren handelt es sich z. B., wenn eine mit Hilfe eines Tabellenkalkulationsprogramms erstellte Datei alle von einer Behörde zu überwachende Betriebe eines bestimmten Wirtschaftszweigs mit Prüfvermerken erfasst, die durch automatisierte Verfahren ausgewertet werden können. Für die Auswertbarkeit kommt es darauf an, ob das System Funktionen enthält, die es ermöglichen, die Dokumentensammlung insgesamt oder das einzelne Dokument nach personenbezogenen Merkmalen zu erschließen (z. B. Zuordnung von Texten zu Personen über Dateiverzeichnisse und Verwaltungsfunktionen, Erschließen von Texten nach Namen und/oder Begriffen).

6. Einen Mustervordruck für die Verfahrensbeschreibung, den ich um eine Muster-Verfahrensbeschreibung ergänzt habe, enthalten die Verwaltungsvorschriften zum NDSG (abgedruckt in Anlage 1). Hierzu einige Anmerkungen:

In der für die o. g. automatisierten Verfahren anzufertigenden Verfahrensbeschreibung sind diverse Angaben einzutragen:

Nr. 1	Name und Anschrift der Daten verarbeitenden Stelle sowie der/des behördlichen Datenschutzbeauftragten.
Nr. 2	Die komplette Bezeichnung, nicht nur die Abkürzung des Verfahrens bzw. der Programme sollte hier eingetragen werden.
Nr. 5	Soweit eine spezielle Rechtsgrundlage mit einem abschließenden Datenkatalog existiert, sind die darin genannten Datenarten aufzuzählen.
Nrn. 6 - 8.1 und 8.2	Im Rahmen allgemeiner Bürokommunikationsanwendungen können die Angaben häufig nur global dargestellt werden.
Nr. 7	Sofern keine spezialgesetzlichen Regelungen vorliegen, ist § 17 NDSG zu beachten.
Nr. 8.3	Die Angaben betreffen Datenübermittlungen an Personen oder Stellen in Staaten außerhalb der EU und des Europäischen Wirtschaftsraums (Island, Liechtenstein, Norwegen). Die Angabe des jeweiligen Staates wird nicht verlangt.

Kommt es zu wesentlichen Änderungen der automatisierten Verfahren, so ist die Verfahrensbeschreibung entsprechend anzupassen. Nur geringfügige Änderungen der Angaben nach § 8 Nr. 3, 4, 5 oder 6 im Mustervordruck erfordern keine sofortige Anpassung. Änderungen der übrigen Angaben erfordern dagegen eine Aktualisierung der Beschreibung.

Die behördlichen Datenschutzbeauftragten haben die Angaben nach § 8 Nrn. 1 bis 6 **jedermann** in geeigneter Weise verfügbar zu machen (§ 8 a Abs. 3 Satz 1), d. h. zur

Einsicht zur Verfügung zu stellen. Hiervon ausgenommen sind die Beschreibungen des Niedersächsischen Verfassungsschutzes und der niedersächsischen Polizei.

§ 8 a
Behördliche Datenschutzbeauftragte

(1) [1]Jede öffentliche Stelle, die personenbezogene Daten automatisiert verarbeitet, hat eine Beauftragte oder einen Beauftragten für den Datenschutz zu bestellen. [2]Mit dieser Aufgabe kann auch eine Person beauftragt werden, die nicht der verarbeitenden Stelle angehört. [3]Ist die Person bereits von einer anderen Stelle zur Beauftragten für den Datenschutz bestellt worden, so setzt die weitere Bestellung das Einvernehmen mit der anderen Stelle voraus.

(2) [1]Bestellt werden darf nur, wer die erforderliche Sachkenntnis und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt mit anderen dienstlichen Aufgaben ausgesetzt ist. [2]Beauftragte sind in dieser Eigenschaft weisungsfrei; sie können sich unmittelbar an die Behördenleitung wenden und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. [3]Sie unterstützen die öffentliche Stelle bei der Sicherstellung des Datenschutzes und wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. [4]Sie sind über geplante Verfahren der automatisierten Verarbeitung personenbezogener Daten zu unterrichten. [5]Sie erhalten eine Übersicht der automatisierten Verarbeitungen mit den Angaben nach § 8 Satz 1. [6]Die öffentlichen Stellen haben die Beauftragten für den Datenschutz bei der Aufgabenerfüllung zu unterstützen.

(3) [1]Die Beauftragten haben auf Antrag die Angaben gemäß § 8 Satz 1 Nrn. 1 bis 6 jedermann in geeigneter Weise verfügbar zu machen. [2]Hiervon ausgenommen sind Beschreibungen nach § 22 Abs. 5 und Beschreibungen für Verarbeitungen zum Zweck der Strafverfolgung. [3]Den Beauftragten obliegt die Vorabprüfung von Verfahren nach § 7 Abs. 3, wobei in Zweifelsfällen die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz zu beteiligen ist. [4]Betroffene können sich unmittelbar an die Beauftragte oder den Beauftragten für den Datenschutz wenden.

(4) Wird in einer öffentlichen Stelle ein Register geführt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse geltend machen, zur Einsichtnahme offen steht, so ist Absatz 1 nur anzuwenden, soweit in dieser öffentlichen Stelle andere automatisierte Verarbeitungen stattfinden.

(5) [1]Die Landesregierung wird ermächtigt, durch Verordnung die Pflicht zur Bestellung einer Beauftragten oder eines Beauftragten für den Datenschutz einzuschränken, soweit in einer öffentlichen Stelle automatisierte Verarbeitungen solche Daten betreffen, bei denen eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung nicht zu erwarten ist. [2]In der Verordnung sind die Zweckbestimmungen der Verarbeitung, die Kategorien der Daten, die

Empfänger, denen die Daten übermittelt werden dürfen, und die Dauer der Aufbewahrung festzulegen.

Zu § 8 a

1. Die gesetzlich bereits 1993 in Niedersachsen eingeführten **behördlichen Datenschutzbeauftragten** stellen neben der zentralen staatlichen Kontrolle durch die oder den Landesbeauftragten ein wichtiges und bewährtes Instrument der **datenschutzrechtlichen Selbstkontrolle** dar. Die EG-Datenschutzrichtlinie hat das Instrument der dezentralen Selbstkontrolle „vor Ort“ aufgegriffen und es den Mitgliedsstaaten in Art. 18 Abs. 2 der Richtlinie gestattet, von der in erster Linie vorgesehenen Verpflichtung zur Meldung automatisierter Verarbeitungen an staatliche Kontrollstellen (sog. **Meldepflicht**) dann abzusehen, wenn durch die Bestellung von **„unabhängigen“** Datenschutzbeauftragten eine den datenschutzrechtlichen Vorgaben entsprechende Verarbeitung der personenbezogenen Daten sichergestellt wird. Da die in der Vergangenheit vorgeschriebenen Dateimeldungen 1997 weitgehend abgeschafft wurden, weil sich die mit ihnen verbundenen Erwartungen nicht erfüllt hatten, kam die Wiedereinführung einer Meldepflicht nicht in Betracht. Der Gesetzgeber war deshalb gehalten, die Stellung der behördlichen Datenschutzbeauftragten entsprechend den Vorgaben der Richtlinie auszugestalten und die Befugnisse der Datenschutzbeauftragten auszuweiten.

Zu Abs. 1

2. Alle öffentlichen Stellen müssen nunmehr eine Beauftragte oder einen Beauftragten für den Datenschutz bestellen, wenn sie personenbezogene Daten automatisiert, d. h. unter Einsatz von Datenverarbeitungsanlagen, verarbeiten. Die bisher geltende Beschränkung, dass eine Bestellung erst dann vorzunehmen ist, wenn in der Regel mindestens fünf Bedienstete ständig personenbezogene Daten automatisiert verarbeiten, ist entfallen.

Als behördliche Datenschutzbeauftragte können auch Personen beauftragt werden, die nicht bei der öffentlichen Stelle beschäftigt sind. Auch bisher schon wurde in Ausnahmefällen die Funktion der Datenschutzbeauftragten insbesondere bei kleineren Dienststellen, die sich aufgrund ihrer personellen und organisatorischen Strukturen nicht in der Lage sahen, eigene Bedienste mit dieser Aufgabe zu betrauen, durch **externe Stellen** wahrgenommen (z. B. durch Bedienstete kommunaler Datenzentralen). Diese Praxis wurde nunmehr gesetzlich abgesichert.

Soweit dies ihre Arbeitskapazitäten zulassen, können behördliche Datenschutzbeauftragte diese Aufgabe auch bei weiteren öffentlichen Stellen wahrnehmen. Dies erfordert selbstverständlich das **Einvernehmen** der Stelle, die die Datenschutzbeauftragten ursprünglich bestellt hat. Auch in diesem Fall ist für die zusätzliche Bestellung ein eigenständiger Bestellungsakt unter Beteiligung der zuständigen Personalvertretung notwendig.

3. Die Bestellung der Beauftragten für den Datenschutz erfolgt durch die Leitung der Behörde oder sonstigen öffentlichen Stelle. Sie sollte aus Gründen der Rechtsklarheit schriftlich vorgenommen werden. In gleicher Weise sollten die Aufgaben, Kontrollbe-

fugnisse und Pflichten der Beauftragten konkretisiert werden (ggf. in der Dienstanweisung über den Datenschutz). Die Bestellung und ggf. auch Abberufung unterliegt gemäß § 67 Abs. 1 Nr. 9 des Niedersächsischen Personalvertretungsgesetzes (NPersVG) der Mitbestimmung des Personalrats.

Es empfiehlt sich gerade in größeren Behörden oder sonstigen Stellen, die in erheblichem Umfang personenbezogene Daten automatisiert verarbeiten, eine sachkundige Vertretung für Fälle der Abwesenheit zu bestellen. Durch die Vertretungsregelung wird eine kontinuierliche Aufgabenwahrnehmung gewährleistet. Verzögerungen bei der Aufgabenerledigung werden vermieden. Dies ist vor allem im Hinblick auf die Bearbeitung von Eingaben und die Vorabkontrolle bei der Einführung oder Änderung automatisierter Verfahren (§ 7 Abs. 3) von Bedeutung.

Zu Abs. 2

4. Zu Datenschutzbeauftragten dürfen nur Personen bestellt werden, die die für die Wahrnehmung der Aufgabe erforderliche **Sachkenntnis** und **Zuverlässigkeit** besitzen. Sachkenntnis ist notwendig auf dem Gebiet der Datenverarbeitung, der behördlichen Organisation und bezüglich der einschlägigen Rechtsvorschriften. Werden zum Zeitpunkt der Bestellung noch nicht alle Voraussetzungen erfüllt, so muss jedenfalls die Bereitschaft und die Fähigkeit vorhanden sein, sich die erforderlichen Kenntnisse umgehend anzueignen. Die öffentliche Stelle ist verpflichtet, für eine entsprechende **Fort- und Weiterbildung** Sorge zu tragen.

In der Regel werden die behördlichen Datenschutzbeauftragten neben ihren Kontrollaufgaben noch weitere Verwaltungsaufgaben wahrnehmen. Dabei ist jedoch zu beachten, dass **Interessenkonflikte** vermieden werden müssen. Die Behördenleitung selbst, die Leitung der Informations- und Kommunikationstechnik bzw. deren Stellvertretung oder von Organisationseinheiten mit intensiver Verarbeitung personenbezogener Daten sollte deshalb nicht zu Datenschutzbeauftragten bestellt werden. Mitarbeiterinnen und Mitarbeiter in Personaldienststellen, die im Rahmen ihrer Funktion sehr viel mit personenbezogenen Daten, insbesondere Personalaktendaten, in Berührung kommen, sowie Mitglieder von Personal- und Schwerbehindertenvertretungen, Gleichstellungs- und Frauenbeauftragte, sollten ebenfalls nicht zu behördlichen Datenschutzbeauftragten ernannt werden, da sie ansonsten in Interessenkonflikte mit anderen dienstlichen Aufgaben geraten könnten. Entsprechendes gilt für IT-Sicherheitsbeauftragte, sofern sie ändernden Zugriff auf die IT-Verfahren haben.

5. Die Behördenleitung ist zwar grundsätzlich in der Entscheidung frei, wie die behördlichen Datenschutzbeauftragten in die Behördenstruktur eingebunden werden. Auf Grund des vermehrten Einsatzes der IuK-Technik und der Anwendung neuer Medien nimmt jedoch die Bedeutung des Datenschutzes und die Signalwirkung für die Öffentlichkeit immer mehr zu. Deshalb dürften die behördlichen Datenschutzbeauftragten insbesondere bei großen Behörden mit hohem Einsatz von IuK-Technik und/oder vielfältiger Verarbeitung personenbezogener Daten im Regelfall unmittelbar bei der Behördenleitung anzusiedeln sein.

Unabhängig von der organisatorischen Einbindung sind die Beauftragten in der Ausübung ihrer Funktion **weisungsfrei**. Sie können sich in ihren Angelegenheiten stets auch ohne Einhaltung eines behördeninternen Dienstweges unmittelbar an die Behördenleitung wenden. Ebenso wie Personalräten, Frauen- oder Gleichstellungsbeauftragten dürfen ihnen auf Grund ihrer Tätigkeit keinerlei berufliche Nachteile entstehen.

6. Nicht nur die Rechtsstellung der behördlichen Datenschutzbeauftragten ist durch die Rechtsänderung gestärkt worden, auch ihre gesetzlichen Aufgaben wurden erweitert. Ihre zentrale Aufgabe wird nach wie vor generalklauselartig als **Unterstützung** der öffentlichen Stellen bei der **Sicherstellung des Datenschutzes** beschrieben. Ergänzend betont das Gesetz, dass die Beauftragten auf die Einhaltung des NDSG, der Datenschutzbestimmungen in anderen Gesetzen und in einschlägigen Verwaltungsvorschriften hinzuwirken haben. Insgesamt wird eine nachhaltige Aufgabenwahrnehmung gefordert. Dies unterstreicht vor allem die EG-Datenschutzrichtlinie. Sie spricht in Art. 18 Abs. 2 von einer Überwachung der Einhaltung der Datenschutzvorschriften durch die Datenschutzbeauftragten und geht ausdrücklich davon aus, dass durch deren Einsatz sichergestellt wird, dass rechtliche Beeinträchtigungen Betroffener durch die Datenverarbeitung verhindert werden.

Zu den Aufgaben der Datenschutzbeauftragten gehören insbesondere die

- **Prüfung**, ob das Gebot der **Datenvermeidung und Datensparsamkeit** (§ 7 Abs. 4) eingehalten wird,
- **Überwachung** der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden,
- **Prüfung**, ob die technischen Maßnahmen (§ 7 NDSG) nach dem jeweiligen Stand der Technik getroffen sind, um eine den Vorschriften des NDSG entsprechende Verarbeitung personenbezogener Daten sicherzustellen,
- **Beteiligung** bei der Vorbereitung von Dienstanweisungen oder Dienstvereinbarungen mit der Personalvertretung einschließlich der Überwachung der Einhaltung dieser Bestimmungen,
- **Schulung** der bei der Verarbeitung personenbezogener Daten tätigen Personen in Grundfragen des Datenschutzes,
- **Beratung** der Behördenleitung sowie einzelner Fachbereiche, Abteilungen und Ämter in Fragen des Datenschutzes und der Datensicherung,
- **Mitwirkung** bei der Festlegung von Anforderungsprofilen für Arbeitsplätze, auf denen sensitive personenbezogene Daten verarbeitet oder genutzt werden,
- **Mitwirkung** bei der Auftragsvergabe und Kontrolle der Umsetzung der datenschutzrechtlichen Vorgaben (§ 6 NDSG) beim Auftragnehmer,
- **Beratung** in den Fragen der sicheren Aktenverwaltung, der informierenden und klaren Formulargestaltung, der datenschutzgerechten Vernichtung von Akten sowie der datenschutzgerechten Löschung von Dateien.

Nach der Entscheidung des Bundesarbeitsgerichts vom 11. November 1997 (NJW 1998, S. 2466) ist der betriebliche Datenschutzbeauftragte nicht berechtigt, die

Datenverarbeitung des Betriebsrats zu kontrollieren. Da streitig ist, ob diese Entscheidung auf behördliche Datenschutzbeauftragte zu übertragen ist, hatte der Landesbeauftragte angeregt, diese Frage im Verlauf des Gesetzgebungsverfahrens eindeutig zu klären. Die Landesregierung hat hierzu bei den Gesetzesberatungen erklärt, nach ihrer Auffassung unterlägen auch die **Personalvertretungen** der Kontrolle der behördlichen Datenschutzbeauftragten. Bei der Ausübung dieser Befugnis sei jedoch der besonderen Stellung der Personalvertretung Rechnung zu tragen. Gleichwohl wäre eine gesetzliche Regelung im NPersVG angebracht.

7. Die behördlichen Datenschutzbeauftragten sind über **geplante Verfahren** der automatisierten Verarbeitung personenbezogener Daten zu unterrichten. Durch die gesetzliche Regelung soll gewährleistet sein, dass Beteiligungen rechtzeitig erfolgen und nicht erst dann, wenn die maßgeblichen Entscheidungen über Beschaffung und Einführung der Verfahren bereits getroffen wurden oder kaum noch revidierbar sind. Den behördlichen Datenschutzbeauftragten ist damit die Möglichkeit eröffnet, bereits im Vorfeld der Einführung automatisierter Verfahren auf datenschutzgerechte Lösungen hinzuwirken. Ist die Beteiligung unterblieben, ist das Vorhaben auszusetzen. Die Beteiligung ist umgehend nachzuholen.

8. Die behördlichen Datenschutzbeauftragten erhalten von den Daten verarbeitenden Stellen (z. B. Fachamt oder zentrale IT-Servicestelle) eine **Übersicht** über die in der Behörde eingerichteten Verfahren zur automatisierten Verarbeitung personenbezogener Daten (§ 8 a Abs. 2 S. 5). Der Übersicht sind die gemäß § 8 Satz 1 zu erstellenden **Verfahrensbeschreibungen** beizufügen (vgl. Anlage 1, Beispiel einer Verfahrensbeschreibung). Die Übersicht, die einen vollständigen Überblick über die in der öffentlichen Stelle betriebenen automatisierten Verfahren geben soll, ist bei der Einführung neuer oder der Änderung bereits eingerichteter Verfahren zeitnah zu aktualisieren. Die Verantwortlichkeit für die Vollständigkeit und Aktualität der Übersicht und der Verfahrensbeschreibungen trägt die Daten verarbeitende Stelle, nicht der behördliche Datenschutzbeauftragte.

9. Die öffentlichen Stellen sind nach Satz 6 nunmehr ausdrücklich verpflichtet, die behördlichen Datenschutzbeauftragten bei ihrer Aufgabenerfüllung zu unterstützen. Der Gesetzgeber hat somit nunmehr eindeutig klargestellt, dass die **Unterstützungspflicht** keine „Einbahnstraße“ darstellt. Dies beinhaltet die für eine effektive Wahrnehmung der Aufgabe angemessene personelle Ausstattung und die Bereitstellung der erforderlichen Sachmittel, z. B. von Räumen, Geräten, Einrichtungen. Der jeweilige Umfang richtet sich nach der Größe der betreffenden Stelle, insbesondere dem Umfang ihrer Datenverarbeitung.

Eine wirksame Aufgabenwahrnehmung erfordert, dass die Datenschutzbeauftragten, sofern sie die Aufgabe nicht hauptamtlich ausüben, im jeweils erforderlichen Umfang von anderen Tätigkeiten entlastet werden. Vor dem Hintergrund, dass der Aufgabenbestand der Datenschutzbeauftragten erheblich ausgeweitet wurde, reicht es künftig nicht mehr aus, diese Aufgabe einem Bediensteten zusätzlich zu seinen sonstigen Aufgaben „zur Erledigung nebenbei“ zu übertragen. Zwar hat der Gesetzgeber der Forderung des Landesbeauftragten, in das Gesetz einen Rechtsanspruch auf

Freistellung im erforderlichen Umfang aufzunehmen, auch im Hinblick auf die Organisationshoheit der Kommunen nicht entsprochen. In der Gesetzesberatung bestand jedoch Einvernehmen darüber, dass den Datenschutzbeauftragten angemessene zeitliche Ressourcen zur Verfügung stehen müssen, um ihre Aufgabe wirksam ausüben zu können. Zwecks Klärung der Frage nach dem Umfang der erforderlichen Freistellung wird den behördlichen Datenschutzbeauftragten empfohlen, schriftlich aufzulisten, welche Aufgaben mit welchen Zeitanteilen im Laufe eines gewissen Zeitraums anfallen, um bei Bedarf einen Nachweis ihrer Tätigkeiten vorlegen zu können.

Zu Abs. 3

10. Die behördlichen Datenschutzbeauftragten sind nach Satz 1 verpflichtet, die gemäß § 8 Satz 1 Nrn. 1 bis 6 in den Verfahrensbeschreibungen festzulegenden Angaben über

- die Bezeichnung der automatisierten Verarbeitung und ihre Zweckbestimmung,
- die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,
- den Kreis der Betroffenen,
- die Art regelmäßig zu übermittelnder Daten, deren Empfänger, in den Fällen des § 6 auch die Auftragnehmer, sowie die Herkunft regelmäßig empfangener Daten,
- die Absicht, Daten in Staaten nach § 14 zu übermitteln,
- Fristen für die Sperrung und Löschung der Daten

auf Antrag **jedermann** in geeigneter Weise, ohne das es hierfür besonderer Voraussetzungen bedarf, verfügbar zu machen. Aus Gründen der Datensicherheit unterbleibt eine Information über die Angaben nach § 8 Satz 1 Nrn. 7 und 8 über die technischen und organisatorischen Maßnahmen sowie über die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

Über die Art und Form der Information entscheiden die behördlichen Datenschutzbeauftragten eigenständig. In der Regel geschieht dies durch eine **Einsichtnahme** bei den Datenschutzbeauftragten vor Ort. Einen Rechtsanspruch auf kostenfreie Übersendung der **Verfahrensbeschreibungen** begründet das Gesetz nicht. Zulässig ist auch eine Veröffentlichung im Internet, wenn sichergestellt ist, dass sich die Informationen auf die Angaben zu Nrn. 1 bis 6 beschränken und Informationen, die zu einer Beeinträchtigung der Verfahrenssicherheit führen könnten, nicht offenbart werden. Ausgenommen von der Einsichtnahme sind Beschreibungen über Datenverarbeitungen nach dem Nds. Verfassungsschutzgesetz, für polizeiliche Aufgaben nach dem Nds. Gesetz für die öffentliche Sicherheit und Ordnung (Nds. SOG) oder für Zwecke der Strafverfolgung.

11. Den Datenschutzbeauftragten ist als wesentliche Aufgabe einer effektiven und bereits im Vorfeld greifenden Datenschutzkontrolle die Durchführung der Vorabprüfung von automatisierten Verfahren nach § 7 Abs. 3, d. h. der Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien

besondere Risiken mit sich bringen, übertragen worden (so genannte **Vorabkontrolle**). Im Ergebnis der unter den Voraussetzungen des § 7 Abs. 3 vor der Inbetriebnahme einer automatisierten Verarbeitung vorzunehmenden Vorabkontrolle ist durch die behördlichen Datenschutzbeauftragten die Feststellung zu treffen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können (vgl. § 7 Anm. 15). Bei behörden- oder ressortübergreifenden Verfahren liegt die Zuständigkeit zur Vorabkontrolle bei der oder dem behördlichen Datenschutzbeauftragten der öffentlichen Stelle, die für die Einführung des Verfahrens verantwortlich ist. Sofern Projektgruppen mit der Einführung landesweiter Verfahren beauftragt worden sind, ist der Projektleiter für die Einbindung des behördlichen Datenschutzbeauftragten verantwortlich.

Den behördlichen Datenschutzbeauftragten sind die für die Durchführung der Vorabkontrolle erforderlichen Unterlagen in geeigneter und prüffähiger Form zur Verfügung zu stellen. Für die Vorarbeiten zur Vorabkontrolle können sie sich der Unterstützung der Daten verarbeitenden Stellen bedienen.

Bestehen im Ergebnis der Vorabkontrolle Zweifel, ob die mit der geplanten automatisierten Verarbeitung verbundenen Risiken wirksam beherrscht werden können, ist die oder der Landesbeauftragte zu beteiligen. Der Einhaltung eines Dienstweges über die Behördenleitung bedarf es nicht. Auch in sonstigen Fragen des Datenschutzes oder der Datensicherheit können die behördlichen Datenschutzbeauftragten die Hilfe der oder des Landesbeauftragten in Anspruch nehmen (vgl. § 19 Abs. 2 NDSG, Anrufung des LfD).

12. Personen, die sich durch die öffentlichen Stelle in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlen, können sich mit ihrem Begehren unmittelbar an die behördlichen Datenschutzbeauftragten wenden. Die Datenschutzbeauftragten nehmen insoweit auf örtlicher Ebene eine **datenschutzrechtliche Ombudsfunktion** ein. Auch die Beschäftigten können sich jederzeit an die behördlichen Datenschutzbeauftragten ihrer öffentlichen Stelle wenden. Zur Wahrung der Vertraulichkeit ist durch organisatorische Maßnahmen sicherzustellen, dass die Eingaben unmittelbar den Beauftragten zugehen.

Die Datenschutzbeauftragten sind verpflichtet, **Eingaben** nachzugehen und bei etwaigen Verstößen in ihrer Behörde darauf hinzuwirken, dass berechtigten Beschwerden abgeholfen wird. Dies gilt auch, wenn Hinweise auf datenschutzrechtliche Verstöße anonym eingereicht werden. Die Weitergabe personenbezogener Daten der Betroffenen (Beschwerdeführer) an die öffentliche Stelle ist statthaft, wenn dies zur Bearbeitung der Eingabe erforderlich ist und schutzwürdige Belange der Betroffenen nicht entgegenstehen. Im Zweifel ist die Einwilligung der Betroffenen einzuholen. Sie sind über das Ergebnis der Überprüfung und die ggf. getroffenen Maßnahmen zu unterrichten. Bei der Eingabenbearbeitung bleibt es den Datenschutzbeauftragten unbenommen, eine von der öffentlichen Stelle abweichende Bewertung der Sach- und Rechtslage vorzunehmen.

Ihre Funktion als Ansprechpartner in allen Angelegenheiten des Datenschutzes können die Datenschutzbeauftragten nur dann wirkungsvoll wahrnehmen, wenn die Öffentlichkeit über diese Aufgabe in geeigneter Weise informiert und der Datenschutzbeauftragte im Internet oder im Organisationsplan der öffentlichen Stelle ausdrücklich aufgeführt wird.

Zu Abs. 4

13. Für öffentliche Stellen, die ausschließlich **Register** führen,

- die zur Information der Öffentlichkeit bestimmt sind und
- entweder jedermann oder allen Personen, die ein berechtigtes Interesse geltend machen, offen stehen, (z. B. Liegenschaftskataster)

entfällt entsprechend den Vorgaben der EG-Datenschutzrichtlinie die Verpflichtung aus Abs. 1 zur Bestellung behördlicher Datenschutzbeauftragter. Dies aber nur dann, wenn in der öffentlichen Stelle keine weiteren automatisierten Verfahren betrieben werden. Der Regelung wird in der Praxis keine weitreichende Bedeutung zukommen, da sich die automatisierte Verarbeitung nur bei wenigen öffentlichen Stellen auf die Führung von Registern beschränken wird.

Zu Abs. 5

14. Absatz 5 ermächtigt die Landesregierung, durch Verordnung **Ausnahmen** von der **Pflicht** zur Bestellung einer oder eines Beauftragten für den Datenschutz zuzulassen, soweit es sich um automatisierte Verarbeitungen handelt, bei denen unter Berücksichtigung der Art der Daten Beeinträchtigungen der Rechte der Betroffenen unwahrscheinlich sind. Nach der als Anlage beigefügten Verordnung vom 10. Juli 2002 (Nds. GVBl. S. 349) entfällt die Pflicht zur Bestellung von Datenschutzbeauftragten für Notarinnen und Notare sowie für Verfahren zur Textverarbeitung einschließlich der Übermittlung elektronischer Dokumente über Telekommunikationsdienste.

Zweiter Abschnitt

Rechtsgrundlagen der Datenverarbeitung

§ 9
Erhebung

(1)[1]Personenbezogene Daten dürfen erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. [2]Die Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. [3]Bei Dritten dürfen personenbezogene Daten nur erhoben werden, wenn

1. **eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,**
2. **die Erhebung zur Abwehr von Gefahren für Leib, Leben oder die persönliche Freiheit erforderlich ist,**
3. **Angaben der Betroffenen überprüft werden müssen,**
4. **offensichtlich ist, dass die Erhebung im Interesse der Betroffenen liegt und sie einwilligen würden,**
5. **die Daten aus allgemein zugänglichen Quellen entnommen werden können, soweit nicht schutzwürdige Interessen der Betroffenen offensichtlich entgegenstehen, oder**
6. **a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder**
   b) die Erhebung bei den Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

(2) [1]Werden Daten bei den Betroffenen erhoben, so sind sie über den Zweck der Erhebung aufzuklären. [2]Werden die Daten auf Grund einer Rechtsvorschrift erhoben, so sind die Betroffenen in geeigneter Weise über diese aufzuklären. [3]Soweit eine Auskunftspflicht besteht oder die Gewährung von Rechtsvorteilen die Angabe von Daten voraussetzt, sind die Betroffenen hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(3) [1]Werden Daten bei einer dritten Person oder einer Stelle außerhalb des öffentlichen Bereichs erhoben, so ist diese auf Verlangen über den Verwendungszweck aufzuklären. [2]Soweit eine Auskunftspflicht besteht, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Zu Abs. 1:

1. Die Vorschrift regelt die erste Phase der Datenverarbeitung. **Datenerhebung** ist das zielgerichtete Beschaffen von Daten, z. B. durch Beobachten, Befragen, Anfordern von Unterlagen. Werden dagegen Daten einer öffentlichen Stelle ohne Aufforde-

rung von Betroffenen oder Dritten zugeleitet (Beispiel: Ein Bürger teilt seiner Gemeinde Beobachtungen mit, um sie zum Einschreiten zu veranlassen) oder kommen sie ihr zufällig zur Kenntnis, handelt es sich nicht um erhobene, sondern um „erlangte Daten“ (vgl. § 10 Abs. 1 Satz 2). Da die öffentliche Stelle bei solchen Daten erstmals bei der Speicherung tätig wird, sind diese erst von dieser Verarbeitungsphase an durch das NDSG geschützt.

2. Die Datenerhebung ist zulässig, wenn die Kenntnis der in Rede stehenden Daten im konkreten Einzelfall zur rechtmäßigen Aufgabenerfüllung der öffentlichen Stelle erforderlich ist. Dazu gehört, dass die Daten erhebende Stelle für die Aufgabe örtlich und sachlich zuständig ist und die rechtlichen Voraussetzungen für ihr Tätigwerden vorliegen.

3. Der **Erforderlichkeitsgrundsatz** ist ein tragendes Gestaltungsprinzip des Datenschutzrechts. Da nach der Rechtsprechung des Bundesverfassungsgerichts jede Verarbeitung personenbezogener Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt (BVerfGE 65, 1, 46), muss die Datenverarbeitung auf das unbedingt notwendige Maß begrenzt werden. Nach der Gesetzesbegründung zu § 9 ist eine Datenverarbeitung deshalb nur erforderlich, wenn die jeweilige Aufgabe ohne das konkrete Datum nicht oder nicht vollständig erfüllt werden kann. Dazu zählt auch, dass die Aufgabe auf andere Weise nur unter unverhältnismäßig großen Schwierigkeiten oder verspätet erfüllt werden könnte (LT-Drs. 12/3290). Es reicht somit nicht aus, wenn die Datenverarbeitung für die Aufgabenwahrnehmung lediglich dienlich oder nützlich ist, zur Abrundung des Bildes beiträgt oder Hintergrundinformationen liefert. Auch eine umfassende **Datenerhebung „auf Vorrat“**, d. h. für den Fall, dass die Daten möglicherweise zu einem späteren Zeitpunkt für eine Aufgabenerfüllung benötigt werden könnten, ist grundsätzlich unzulässig und nur auf bestimmte Anlässe der Strafverfolgung beschränkt (s. u. a. Beschlüsse des BVerfG, 1 BvR 370/07/1 BvR 595/07 vom 27. Februar 2008 sowie 1 BvR 256/08 vom 11. März 2008 und 1 BvR 256/08 vom 28. Oktober 2008).

Nach dem **Transparenzgebot** des Bundesverfassungsgerichts, das davon ausgeht, dass die Bürgerinnen und Bürger grundsätzlich wissen können müssen, „wer, was, wann und bei welcher Gelegenheit über sie weiß“ (BVerfGE 65, 1, 44), sind Daten grundsätzlich bei den Betroffenen mit ihrer Kenntnis zu erheben. Nur diese Verfahrensweise gibt ihnen die Möglichkeit, selbst über Preisgabe und Verwendung ihrer Daten zu bestimmen. Eine Datenerhebung „hinter dem Rücken“ der Betroffenen ist nach dem allgemeinen Datenschutzrecht nicht zulässig. Beispiel: Angaben über den Arbeitsverdienst darf die Behörde nicht beim Arbeitgeber erfragen, sie muss sich an den Arbeitnehmer selbst wenden.

4. In den in Abs. 1 Satz 3 genannten Fällen hat der Gesetzgeber nach einer Abwägung zwischen den verfolgten Verwaltungsinteressen und dem Persönlichkeitsrecht der Betroffenen ausnahmsweise eine **Datenerhebung bei Dritten** zugelassen, ohne dass die Betroffenen davon Kenntnis erhalten. Im Einzelnen ist dazu zu bemerken:

Nr. 3: Eine **Überprüfung von Angaben des Betroffenen** kommt nur in Betracht, wenn im Einzelfall tatsächliche Anhaltspunkte dafür bestehen,

dass von ihm gemachte Angaben unrichtig sind. Auch belegbare Verwaltungseinschätzungen, dass in einem bestimmten Aufgabenfeld (z. B. der Subventionsgewährung) häufig mit betrügerischen Angaben gerechnet werden muss, erlauben dagegen noch keine Datenerhebung bei Dritten. Die Anhaltspunkte, die Anlass zur Überprüfung gegeben haben, hat die Daten verarbeitende Stelle festzuhalten.

Nr. 4: Auch wenn diese Form der Datenerhebung nach verständiger Einschätzung **im Interesse des Betroffenen** liegt, kommt sie nicht in Betracht, wenn dieser zu erkennen gegeben hat, dass er mit einer Datenerhebung bei Dritten nicht einverstanden ist.

Nr. 5: Auf **Daten aus allgemein zugänglichen Quellen** darf nur zurückgegriffen werden, soweit nicht schutzwürdige Interessen der Betroffenen offensichtlich entgegenstehen. Damit wird berücksichtigt, dass in Einzelfällen bei sensiblen Daten die Rechtfertigung der Datenverarbeitung mit einer lange zurückliegenden Veröffentlichung, die möglicherweise selbst problematisch war, auf Bedenken stoßen kann, weil diese Veröffentlichung den Schutz der Daten für den Betroffenen auf Dauer aufheben würde.

Nr. 6: Nach Buchst. a) kommt eine Erhebung bei Dritten in Frage, wenn die zu erfüllende **Aufgabe ihrer Art nach** eine **solche Erhebung erfordert**. Da der wichtigste Fall dieser Art, eine Dritterhebung zur Überprüfung von Angaben des Betroffenen, bereits in Nr. 3 geregelt ist, ist der Anwendungsbereich der Vorschrift gering. Denkbar sind vor allem Vorgänge, bei denen eine Datenerhebung beim Betroffenen die notwendige Aufklärung des Sachverhalts schwerwiegend behindern oder vereiteln würde. Dies ist z. B. bei der Aufklärung eines Dienstvergehens im Rahmen des Disziplinarrechts denkbar.

Buchst. b) lässt eine Erhebung bei Dritten zu, wenn die **Erhebung beim Betroffenen** einen **unverhältnismäßigen Aufwand** erfordern würde. Damit nicht bloße finanzielle Erwägungen die Grundrechtsposition des Betroffenen beschneiden, müssen an das Vorliegen dieser Voraussetzung hohe Anforderungen gestellt werden. Je schutzwürdiger die zu erhebenden Daten sind, desto größer ist der in Kauf zu nehmende Aufwand einer Datenerhebung beim Betroffenen. Bei der vorzunehmenden Abwägung sind neben der Art der Daten vor allem der Zeit- und Kostenaufwand der Erhebung beim Betroffenen im Verhältnis zu einer Dritterhebung von Bedeutung.

In beiden Fallvarianten (Buchst. a und b) dürfen darüber hinaus keine Anhaltspunkte dafür bestehen, dass durch die Dritterhebung schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

5. Werden Daten unter Verstoß gegen Abs. 1 erhoben (z. B. indem eine Behörde nicht erforderliche Daten erhebt oder unzulässigerweise eine Datenerhebung bei

Dritten vornimmt), dürfen diese Daten nicht gespeichert werden. Die **Speicherung** ist zur rechtmäßigen Aufgabenerfüllung im Sinne des § 10 Abs. 1 Satz 1 nicht erforderlich. Kommt es dennoch zu einer Speicherung, sind die Daten nach § 17 Abs. 2 Nr. 1 von Amts wegen zu löschen.

Zu Abs. 2 und 3:

6. Die **Hinweis- und Aufklärungspflichten** sollen die Betroffenen in die Lage versetzen, ihre Rechte sachgemäß wahrzunehmen. Art und Umfang der Hinweise richten sich nach den jeweiligen Umständen. Ist der Zweck ohne weiteres und zweifelsfrei erkennbar, kann ein entsprechender Hinweis ausnahmsweise entbehrlich sein. Im Übrigen kann er von der Angabe eines bloßen Stichworts bis zu einer näheren Erläuterung reichen. Die Aufklärung muss in einer für den Betroffenen verständlichen Weise erfolgen. Bei einer schriftlichen Befragung sollte auch die Aufklärung schriftlich vorgenommen werden. Der Hinweis auf die Rechtsgrundlage der Datenerhebung muss so gefasst sein, dass der Betroffene die Rechtslage nachprüfen kann. Dazu wird in der Regel eine Bezeichnung des Gesetzes, außer bei allgemein bekannten Gesetzen (wie dem BGB und dem StGB), die Angabe der Fundstelle und die Nennung der einschlägigen Vorschrift gehören. Von besonderer Bedeutung ist der Hinweis, ob eine Auskunftspflicht besteht, oder ob die Auskunft in der freien Entscheidung des Betroffenen steht. Eine Unklarheit hierüber darf beim Betroffenen nicht zurückbleiben. Bei der Gestaltung von Fragebogen sind Fragen, deren Beantwortung freiwillig ist, in eindeutiger Weise zu kennzeichnen.

Ein Verstoß gegen die Aufklärungspflichten macht die Datenerhebung nicht ohne weiteres unwirksam und hindert die weitere Datenverarbeitung damit grundsätzlich nicht. Anders ist die Rechtslage, wenn der Hinweis auf die Freiwilligkeit unterlassen wurde. In diesem Fall dürfen die erhobenen Daten nicht gespeichert werden, sie sind vielmehr von Amts wegen zu löschen (§ 17 Abs. 2 Nr. 1).

7. Hinsichtlich der Datenerhebung durch Videobeobachtung von nicht öffentlich zugänglichen Räumen wird auf die Erläuterungen zu § 25 a verwiesen.

§ 10
Speicherung, Veränderung, Nutzung; Zweckbindung

(1) [1]Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und die Daten für diese Zwecke erhoben worden sind. [2]Erlangt die öffentliche Stelle Kenntnis von personenbezogenen Daten, ohne diese erhoben zu haben, so darf sie diese Daten nur für Zwecke verarbeiten, für die sie diese Daten erstmals speichert.

(2) [1]Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig,

1. **wenn die Betroffenen eingewilligt haben,**
2. **in den Fällen des § 9 Abs. 1 Satz 3 Nrn. 1 bis 5 oder**
3. **wenn sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten ist.**

[2]Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, so dürfen sie für andere Zwecke nur gespeichert, verändert oder genutzt werden, wenn die Betroffenen eingewilligt haben oder wenn eine Rechtsvorschrift dies zulässt.

(3) [1]Ein Speichern, Verändern oder Nutzen zu anderen Zwecken liegt nicht vor, wenn dies zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen erfolgt. [2]Zulässig ist auch die Verarbeitung zu Ausbildungs- und Prüfungszwecken, soweit nicht berechtigte Interessen der Betroffenen an der Geheimhaltung der Daten offensichtlich überwiegen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verarbeitet werden.

Zu Abs. 1

1. Die Vorschrift regelt die auf die Datenerhebung folgenden Verarbeitungsschritte der Datenspeicherung, -veränderung und -nutzung (zu diesen Begriffen s. § 3 Abs. 2). Sie zeigt das grundlegende Regelungsmuster datenschutzrechtlicher Befugnisnormen: Die Verarbeitung ist zulässig, wenn sie 1. zur Aufgabenerfüllung der

öffentlichen Stelle erforderlich ist und 2. zu dem Zweck erfolgt, für den die Daten erhoben worden sind.

2. Das damit angesprochene **Zweckbindungsprinzip** ist für die Verarbeitung personenbezogener Daten von ebenso zentraler Bedeutung wie das Erforderlichkeitsprinzip. Die Zweckbindung verhindert, dass öffentliche Stellen bei ihnen vorhandene Daten multifunktional verwenden dürfen. Beispiel: Eine Kämmerei darf Daten über Gemeindebedienstete, die ihrer Verpflichtung zur Hundesteuerzahlung nicht nachkommen, nicht an die Personalstelle der eigenen Behörde weitergeben, damit diese die Beschäftigten zur Zahlung veranlassen. Wäre eine zweckändernde Verarbeitung allgemein zulässig, könnte das Recht der Betroffenen, selbst über Preisgabe und Verwendung ihrer Daten zu bestimmen, nicht mehr gewährleistet werden.

Der Zweck der Datenverarbeitung folgt aus der jeweiligen Fachaufgabe. Bei einer vorausgegangenen Datenerhebung ergibt sich der Zweck aus dem Hinweis der öffentlichen Stelle gegenüber dem Betroffenen bzw. dem Dritten (§ 9 Abs. 2 und 3). Sofern Daten ohne Erhebung der öffentlichen Stelle zur Kenntnis gelangt sind, legt sie den Zweck bei der erstmaligen Speicherung fest. Organisationseinheiten oder deren Teile, die innerhalb einer Behörde unterschiedliche Aufgaben wahrnehmen, verarbeiten Daten zu verschiedenen Zwecken. Eine Datenweitergabe zwischen solchen Stellen führt zu einer Zweckänderung. Organisationseinheiten, die bloße Hilfsfunktionen der jeweiligen Fachaufgabe wahrnehmen, wie z. B. ein zentraler Schreibdienst, nehmen dagegen keinen von der Fachaufgabe zu unterscheidenden Zweck wahr.

Zu Abs. 2

3. Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck (**Zweckänderung** oder **Zweckdurchbrechung**) kommt nur in den in der Vorschrift genannten sieben Fällen in Betracht. Sie entsprechen weitgehend den Voraussetzungen, unter denen nach § 9 Abs. 1 Satz 3 eine Datenerhebung bei Dritten zugelassen ist.

4. Eine verstärkte Zweckbindung besteht für Daten, die einem **Berufs**- oder **besonderen Amtsgeheimnis** unterliegen und die der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind. Berufsgeheimnisse sind Geheimnisse, die den Angehörigen der in § 203 Abs. 1 StGB genannten Berufsgruppen (u. a. Ärzte, Berufspsychologen, Rechtsanwälte, Ehe-, Erziehungs- oder Jugendberater, Suchtberater, Sozialarbeiter) in Ausübung ihrer Tätigkeit bekannt werden. Besondere Amtsgeheimnisse sind solche Geheimnisse, die über das im Verwaltungsverfahrensrecht geregelte allgemeine Amtsgeheimnis und die dienst- und arbeitsrechtlichen Verschwiegenheitspflichten hinausgehen (wie das Steuergeheimnis, das Post- und Fernmeldegeheimnis oder das Statistikgeheimnis). Bei diesen Daten ist eine Zweckänderung nur zulässig, wenn eine Einwilligung des Betroffenen vorliegt oder eine besondere Rechtsvorschrift dies erlaubt.

Zu Abs. 3

5. Für die in der Vorschrift genannten Aufgaben, die an sich einen anderen Verarbeitungszweck betreffen, bestimmt das Gesetz wegen der ganz überwiegend vorhandenen Nähe zur jeweiligen Fachaufgabe, dass eine Zweckänderung nicht vorliegt (**Fiktion der Zweckidentität**).

Aufsichts- und Kontrollbefugnisse bestehen im Rahmen der Dienst-, Fach- oder Rechtsaufsicht, sie können innerhalb einer Behörde, im Verhältnis zu einer nachgeordneten Behörde oder gegenüber öffentlichen Stellen in privater Rechtsform (z. B. Beliehene) wahrgenommen werden.

Eines Rückgriffs auf Abs. 3 bedarf es nicht in Bezug auf die Kontrolle durch Fachvorgesetzte innerhalb der für die Aufgabenerledigung zuständigen Organisationseinheit, da diese zum Primärzweck gehört.

Soweit spezialgesetzliche Regelungen aufsichtführenden oder kontrollierenden Stellen Informationszugangs- und Verwertungsrechte einräumen, stellt sich das Problem der Zweckbindung infolge des Vorrangs gemäß § 2 Abs. 6 NDSG nicht mehr. Dies gilt z. B. sowohl für die in Satz 1 gesondert aufgeführte Rechnungsprüfung als auch für die Kommunalaufsicht (vgl. u. a. § 95 LHO, §§ 153 ff. NKomVG i. V. m. § 3 Abs. 2 NKPG).

Organisationsuntersuchungen betreffen die Aufbau- und Ablauforganisation. Sie können innerhalb der betroffenen Behörde von einer dazu befugten vorgesetzten Stelle, aber auch von einem dafür eingesetzten Beratungsunternehmen durchgeführt werden.

Bei der Verwendung von personenbezogenen Daten für **Ausbildungs- und Prüfungszwecke** wird die Zweckidentität nicht in gleicher Weise fingiert wie in den übrigen Fällen. Zur Wahrung der Belange der Betroffenen darf hier eine Verarbeitung nur nach einer Abwägung mit den berechtigten Interessen der Betroffenen an der Geheimhaltung der Daten erfolgen. Dies ist insbesondere bei der Bearbeitung von Personalvorgängen sowie von Steuerdaten durch Auszubildende zu beachten.

Das **Erforderlichkeitsprinzip** ist selbstverständlich auch in den vorgenannten Fällen zu beachten.

Zu Abs. 4

6. Ein striktes **Verbot der Zweckänderung** besteht für Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

§ 10 a
Automatisierte Einzelentscheidung

(1) Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

(2) [1]Dies gilt nicht, wenn

1. **eine Rechtsvorschrift dies vorsieht,**
2. **dem Begehren der Betroffenen stattgegeben wurde oder**
3. **die Wahrung der berechtigten Interessen der Betroffenen durch geeignete Maßnahmen gewährleistet und den Betroffenen von der verantwortlichen Stelle die Tatsache, dass eine Entscheidung nach Absatz 1 vorliegt, mitgeteilt wird.**

[2]Als geeignete Maßnahme im Sinne der Nummer 3 gilt insbesondere die Möglichkeit der Betroffenen, ihren Standpunkt geltend zu machen; die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

(3) Das Recht der Betroffenen auf Auskunft nach § 16 erstreckt sich in den Fällen des Absatzes 1 auch auf den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten.

Zu Abs. 1

1. Die Vorschrift setzt Art. 15 der EG-Datenschutzrichtlinie um. Sie entspricht § 6 a BDSG. Die Regelung soll gewährleisten, dass Entscheidungen, bei denen eine **Bewertung von Persönlichkeitsmerkmalen** vorgenommen wird, nicht ausschließlich durch eine technische Vorrichtung getroffen, sondern immer von einem Menschen verantwortet werden. Dieser Gedanke kommt bereits in § 95 Abs. 4 NBG zum Ausdruck. Danach dürfen Beurteilungen sowie dienstrechtliche Entscheidungen nicht ausschließlich auf Erkenntnisse gestützt werden, die unmittelbar durch eine automatisierte Datenverarbeitung gewonnen werden. Die Entscheidung nach § 10 a muss sich auf eine Bewertung einzelner Persönlichkeitsmerkmale beziehen. Dabei muss es sich um Angaben von einer gewissen Komplexität handeln, bloße Messwerte (wie die Angabe des Blutalkoholgehalts) reichen nicht aus. Sie sind für eine Bewertung im Sinne dieser Vorschrift nicht geeignet. Als Beispiele für die angesprochenen Persönlichkeitsmerkmale nennt die EG-Datenschutzrichtlinie die berufliche Leistungsfähigkeit, die Zuverlässigkeit oder das Verhalten einer Person.

Den Einsatz automatisierter Datenverarbeitung zur Vorbereitung oder Unterstützung einer Entscheidung, die sich auf entsprechende Persönlichkeitsmerkmale bezieht,

schließt die Vorschrift nicht aus. Eine Vorauswahl geeigneter Personen nach bestimmten Kriterien ist deshalb im Wege der automatisierten Datenverarbeitung durchaus möglich. Ausschlaggebend ist, dass die abschließende Entscheidung von einer Person verantwortet wird.

Zu Abs. 2

2. Zulässig ist eine **automatisierte Einzelentscheidung** allerdings, wenn eine Rechtsvorschrift oder eine andere der in dieser Bestimmung genannten Voraussetzungen vorliegt, mit denen den Interessen des Betroffenen Rechnung getragen wird. Dazu gehört insbesondere, dass der Betroffene die Möglichkeit hat, seinen Standpunkt in der Sache geltend zu machen.

Zu Abs. 3

3. In den von der Vorschrift erfassten Fällen wird dem Betroffenen ein erweitertes **Auskunftsrecht** eingeräumt. Dieses Recht wird in § 10 a Abs. 3 und § 16 Abs. 1 Satz 1 Nr. 4 unterschiedlich beschrieben. § 10 a spricht von einer Auskunft über den logischen Aufbau der automatisierten Verarbeitung dieser Daten, § 16 von einer Auskunft über Art und Struktur der automatisierten Verarbeitung. Einen unterschiedlichen Regelungsgehalt weisen die Vorschriften jedoch nicht auf. Die Auskunft muss dem Betroffenen deutlich machen, in welcher Weise aus seinen Daten eine Bewertung von Persönlichkeitsmerkmalen abgeleitet wird.

4. § 10 a enthält Unstimmigkeiten, die in der EG-Datenschutzrichtlinie bereits angelegt sind. So ist nicht ersichtlich, warum das Verbot der automatisierten Einzelentscheidung nicht auf Entscheidungen beschränkt worden ist, die nachteilige Auswirkungen für die Betroffenen haben, sondern auch solche Entscheidungen einbezogen werden, die für die Betroffenen eine positive Rechtsfolge nach sich ziehen. Auf die Regelungen des Verwaltungsverfahrensrechts ist die Vorschrift nicht abgestimmt. § 28 VwVfG i. V. m. § 1 Abs. 1 NVwVfG schreiben die Anhörung des Beteiligten vor Erlass eines belastenden Verwaltungsakts vor.

§ 11
Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nur zulässig, wenn die Übermittlung zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen.

(2) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten der Betroffenen oder Dritter in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der Betroffenen oder Dritter an deren Geheimhaltung offensichtlich überwiegen; eine weitere Verarbeitung dieser Daten ist unzulässig.

(3) [1]Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. [2]Erfolgt die Übermittlung auf Grund eines Ersuchens, so hat die übermittelnde Stelle lediglich zu prüfen, ob sich das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden Stelle hält. [3]Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; die empfangende Stelle hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. [4]Erfolgt die Übermittlung durch automatisierten Abruf (§ 12), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs die empfangende Stelle.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

Zu Abs. 1

1. Eine **Datenübermittlung** (zum Begriff s. § 3 Abs. 2 Nr. 4) innerhalb des öffentlichen Bereichs ist im Kern unter den gleichen Voraussetzungen zulässig, wie die Datenspeicherung, Veränderung und Nutzung. Die Übermittlung muss zur **Aufgabenerfüllung** (der übermittelnden oder der empfangenden Stelle) erforderlich sein und sie muss im Rahmen der **Zweckbindung** erfolgen. Ist Letzteres nicht der Fall, müssen die Voraussetzungen für eine **Zweckänderung** (§ 10 Abs. 2) vorliegen.

2. Die Regelung gilt für die Datenweitergabe an andere öffentliche Stellen innerhalb der Bundesrepublik Deutschland, der EU und der übrigen Vertragsstaaten des Europäischen Wirtschaftsraums (Island, Liechtenstein, Norwegen). Nach Abs. 4 ist sie auf die Datenweitergabe innerhalb einer öffentlichen Stelle, die datenschutzrechtlich nicht als Übermittlung, sondern als Nutzung (§ 3 Abs. 2 Nr. 7) anzusehen ist, da keine Weitergabe an eine dritte Stelle vorliegt, entsprechend anzuwenden. Eine

Datenübermittlung ist auch im Falle eines Datenabgleichs durch eine dritte Stelle gegeben.

Von der Vorschrift wird die Übermittlung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (s. dazu Erläuterungen zu § 10 Abs. 2), nicht erfasst. Wegen der Tiefe des damit verbundenen Rechtseingriffs müssen die Voraussetzungen für eine Übermittlung dieser Daten bereichsspezifisch geregelt werden.

3. Bei der Bearbeitung eines Verwaltungsvorgangs sind die Phasen der Datenerhebung und der Datenübermittlung in der Regel miteinander verbunden. Ein **Auskunftsersuchen** einer Behörde an eine andere stellt eine Datenerhebung (bei Dritten) dar, deren Zulässigkeit sich nach § 9 richtet. Die Antwort der angesprochenen Behörde wiederum ist als Datenübermittlung nach § 11 i. V. m. den Zweckbindungsvorschriften des § 10 zu beurteilen.

4. Zur Aufgabenerfüllung der übermittelnden Stelle ist die Datenübermittlung insbesondere dann erforderlich, wenn diese Auskunfts-, Benachrichtigungs- oder Beteiligungspflichten hat. Für die Beurteilung der Erforderlichkeit beim Empfänger spielt es grundsätzlich keine Rolle, ob sich dieser die Daten auch auf andere Weise verschaffen könnte; allerdings hat er den Vorrang der Datenerhebung beim Betroffenen (§ 9 Abs. 1 S. 2 und 3) zu beachten. Die Zweckbindung der übermittelten Daten setzt sich beim Empfänger fort. Auch er darf die Daten nur zu dem Zweck verarbeiten, zu dem sie ihm übermittelt worden sind. Liegen die Voraussetzungen für eine Zweckänderung (§ 10 Abs. 2) vor, dürfen die Daten allerdings auch für vom Übermittlungszweck abweichende Zwecke verarbeitet werden.

Zu Abs. 2

5. Die Vorschrift enthält für die Übermittlung von Daten in Akten eine Einschränkung des Erforderlichkeitsprinzips (sog. **Aktenprivileg**). Eine strikte Einhaltung des Erforderlichkeitsprinzips würde eine intensive Durchsicht der Akten und eine Löschung jedes personenbezogenen Datums, das für die Aufgabenerledigung der empfangenden Stelle nicht erforderlich ist, notwendig machen. Wegen der bei einer solchen Verfahrensweise kaum zu bewältigenden verwaltungspraktischen Probleme lässt das Gesetz es zu, dass für den Fall, dass eine Trennung der erforderlichen Daten des Betroffenen von weiteren nicht erforderlichen Daten nicht oder nur mit unvertretbarem Aufwand vorgenommen werden kann, auch die zur Aufgabenerfüllung nicht erforderlichen Daten übermittelt werden dürfen. Dies setzt allerdings voraus, dass berechtigte Interessen der Betroffenen oder Dritter an der Geheimhaltung nicht überwiegen. Um das **Trennungsgebot** nicht leer laufen zu lassen, sind die öffentlichen Stellen gehalten, ihre Aktenführung so einzurichten, dass eine Aktentrennung möglichst erreicht werden kann, z. B. durch Bildung von Teil- oder Unterakten. Für **Personalakten** sind z. B. durch Gesetz geeignete Regelungen getroffen worden.

Für die zulässigerweise übermittelten, zur Aufgabenerfüllung aber nicht erforderlichen Daten in Akten gilt ein striktes **Verwertungsverbot**.

Zu Abs. 3

6. Die Verantwortung für die datenschutzrechtliche Zulässigkeit von Datenflüssen zwischen öffentlichen Stellen trägt grundsätzlich die übermittelnde Stelle, die die Verfügungsgewalt über die bei ihr vorhandenen Daten besitzt.

Erfolgt die Übermittlung dagegen auf Ersuchen einer öffentlichen Stelle, hat letztlich nur diese die fachliche Kompetenz, die Erforderlichkeit der Daten zur Aufgabenerledigung zuverlässig zu beurteilen. Der ersuchenden Stelle weist das Gesetz deshalb die Verantwortung für die Rechtmäßigkeit der Übermittlung in solchen Fällen zu. Die übermittelnde Stelle hat bei einer Übermittlung auf Ersuchen nur zu prüfen, ob die ersuchende Stelle örtlich und sachlich für die Erfüllung der Aufgabe zuständig ist, für die sie die Daten anfordert (sog. Schlüssigkeitsprüfung). Diese Prüfung wird erleichtert, wenn die anfragende Stelle im Ersuchen hierzu bereits entsprechende Angaben macht. Nur wenn im Einzelfall Zweifel an der Rechtmäßigkeit des Ersuchens bestehen, hat die ersuchte Stelle diese Frage umfassend zu prüfen. Sofern die Voraussetzungen der Amtshilfe erfüllt sind, wird aus der Übermittlungsbefugnis eine Übermittlungspflicht.

§ 12
Automatisiertes Abrufverfahren

(1) [1]Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf eines Dritten ermöglicht, darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies zulässt. [2]Die Zulässigkeit des einzelnen Abrufs bestimmt sich nach den Vorschriften dieses Gesetzes.

(2) [1]Die Landesregierung wird ermächtigt, durch Verordnung für die Behörden und Einrichtungen des Landes sowie für die der Aufsicht des Landes unterliegenden sonstigen öffentlichen Stellen die Einrichtung automatischer Abrufverfahren zuzulassen. [2]Für die Zulassung solcher Verfahren innerhalb des Geschäftsbereichs eines Ministeriums wird das jeweilige Ministerium ermächtigt, die Verordnung zu erlassen. [3]Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung der schutzwürdigen Interessen des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. [4]In der Verordnung sind die Datenempfänger, die Art der zu übermittelnden Daten, der Zweck des Abrufs sowie die wesentlichen bei den beteiligten Stellen zu treffenden Maßnahmen zur Kontrolle der Verarbeitung festzulegen. [5]Die Landesbeauftragte für den Datenschutz oder der Landesbeauftragte für den Datenschutz (die Landesbeauftragte oder der Landesbeauftragte) ist vorher zu hören.

(3) Sind automatisierte Abrufverfahren in einer Verordnung nach Absatz 2 zugelassen, so dürfen sie auf Verlangen des Landesrechnungshofs auch für die Rechnungsprüfung eingesetzt werden.

(4) [1]Personenbezogene Daten dürfen nicht zum Abruf durch Personen oder Stellen außerhalb des öffentlichen Bereichs bereitgehalten werden. [2]Dies gilt nicht für den Abruf durch Betroffene.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus solchen Datenbeständen, die jeder Person offen stehen oder deren Inhalt veröffentlicht werden darf.

Zu Abs. 1

1. Aus der Sichtweise des Datenschutzes bringen **automatisierte Abrufverfahren** eine besondere Gefährdung für das Persönlichkeitsrecht des Betroffenen mit sich. Die Daten abrufende Stelle kann über den gesamten Datenbestand verfügen, ohne dass die speichernde Stelle auf den einzelnen Abruf Einfluss nehmen kann. Dadurch besteht die Gefahr einer unbegrenzten Datenweitergabe und –verwendung. Deshalb wird die Einrichtung solcher Verfahren nur durch Rechtsvorschrift zugelassen.

Die Regelung gilt nicht für

- Online-Anschlüsse, mit denen keine personenbezogenen, sondern statistische Daten übermittelt werden,

- Abrufverfahren **innerhalb einer Daten verarbeitenden Stelle**, da eine solche Datenweitergabe keine Übermittlung, sondern eine Nutzung darstellt (vgl. Erläuterung Nr. 2 zu § 3),
- Datenflüsse im Rahmen einer Datenverarbeitung im Auftrag, da der Auftragnehmer nicht als Dritter anzusehen ist (§ 3 Abs. 4 Satz 3), sondern als Bestandteil der Daten verarbeitenden Stelle,
- den Abruf von Daten aus den Ratsinformationssystemen der Kommunen, da Mandatsträger sowie sonstige berechtigte Personen keinen Zugriff auf den gesamten Datenbestand der Kommune haben, sondern nur die von der Kommune für sie zusammengestellten Sitzungsunterlagen einsehen bzw. abrufen (Zugriffsberechtigung) können.

Ist ein automatisiertes Abrufverfahren durch Rechtsvorschrift eingerichtet worden, müssen für jeden Einzelabruf zusätzlich die Voraussetzungen nach dem NDSG erfüllt sein. Zu prüfen ist somit neben der Zulässigkeit des Verfahrens (§ 12) auch die Zulässigkeit des Abrufs im Einzelfall (z. B. §§ 9 ff.). Die Verantwortung für die Rechtmäßigkeit des Abrufs trägt die abrufende Stelle (§ 11 Abs. 3).

2. Voraussetzung für den Erlass einer entsprechenden Rechtsvorschrift ist, dass das Abrufverfahren nach einer Abwägung zwischen dem Recht auf informationelle Selbstbestimmung und den Aufgaben der beteiligten Stellen als angemessen anzusehen ist. Im Rahmen dieser Abwägung ist zu berücksichtigen, dass die Datenübermittlungen dem Grunde nach zulässig sein müssen. Auch die Zweckbindung muss beachtet werden. Von Bedeutung ist auch, ob es sich um besonders sensible Daten handelt und inwieweit deren Verarbeitung nachteilige Auswirkungen auf die Betroffenen haben kann. Auf Seiten der öffentlichen Stellen sind in die Abwägung u. a. einzubeziehen ein besonderes Interesse an einem schnellen Datenaustausch, die Häufigkeit entsprechender Übermittlungen und das Vorliegen von Massenverfahren. Wirtschaftliche Erwägungen werden bei der Einrichtung entsprechender Verfahren in der Regel eine wesentliche Rolle spielen, auf sie allein kann die Einrichtung eines Verfahrens jedoch nicht gestützt werden.

Neben den Datenempfängern, der Art der zu übermittelnden Daten und dem Zweck des Abrufs sind die bei den beteiligten Stellen wesentlichen Kontrollmaßnahmen in der Verordnung festzulegen. Dazu gehören insbesondere Protokollierungspflichten, um stichprobenartige Überprüfungen der Abrufe zu ermöglichen. Vor Erlass einer Rechtsverordnung ist die oder der Landesbeauftragte für den Datenschutz zu hören.

Soweit entsprechende Verfahren im Rahmen der Wahrnehmung von Aufgaben des übertragenen Wirkungskreises von Gemeinden, Landkreisen und sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts eingerichtet werden sollen, ist hierfür ebenfalls eine Verordnung erforderlich.

Sollen automatisierte Abrufverfahren zur Wahrnehmung von Aufgaben des eigenen Wirkungskreises eingerichtet werden, können diese nach § 12 Abs. 1 in Verbindung mit der satzungsbegründenden Rechtsvorschrift durch Satzung zugelassen werden.

Der Landesbeauftragte für den Datenschutz ist **vor dem Erlass einer solchen Satzung anzuhören.**

Auf Nr. 13.2 der als Anlage beigefügten Verwaltungsvorschriften zum NDSG wird verwiesen.

Zu Abs. 4

3. Ein Abruf darf nur von öffentlichen Stellen erfolgen. Private sollen keinen automatisierten Zugriff auf personenbezogene Datenbestände der öffentlichen Verwaltung haben. Nur für einen Abruf der Betroffenen gilt dies nicht.

Zu Abs. 5

4. Für Datenbestände, in die jede Person Einsicht nehmen kann, und für Daten, die veröffentlicht werden dürfen, gilt die Regelung nicht. Bei solchen Datenbeständen, die jedermann zugänglich sind, führt ein automatisiertes Abrufverfahren nicht zu einer besonderen Gefährdung des Persönlichkeitsrechts der Betroffenen. Hierzu zählen z. B. allgemeine, für jedermann zugängliche Informationen in Ratsinformationssystemen, die der allgemeinen Öffentlichkeit z. B. auch per Internetportal der Kommunen zur Verfügung gestellt werden.

§ 13
Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

1. **sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen,**
2. **die Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt, oder**
3. **sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben.**

In den Fällen des Satzes 1 Nr. 3 sind die Betroffenen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten.

(2) Die übermittelnde Stelle hat die Empfänger zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie ihnen übermittelt wurden.

Zu Abs. 1

1. Eine Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs kann sich an natürliche Personen bzw. alle Stellen des privaten Rechts richten. Dazu gehören auch die Unternehmen, die unter § 2 Abs. 3 fallen (**Wettbewerbsunternehmen**).

Eine Datenübermittlung in den privaten Bereich kommt in drei Fällen in Betracht.

Zu Abs. 1 Nr. 1

Die Übermittlung ist zulässig, wenn sie zur **Aufgabenerfüllung der übermittelnden Stelle** erforderlich ist und die Übermittlung im Rahmen der Zweckbindung der Daten oder einer zulässigen Zweckänderung liegt. Dieser Tatbestand entspricht der Grundregel des § 11. Hierbei handelt es sich zumeist um Fälle, in denen eine **Auskunftspflicht** der öffentlichen Stelle besteht oder um solche Fälle, in denen die öffentliche Stelle selbst ein Auskunftsersuchen an private Stellen richtet und zur Begründung dieses Ersuchens gehalten ist, personenbezogene Angaben zu machen. Beispiel: Mit Zustimmung des Betroffenen bittet eine Behörde dessen Arbeitgeber um Auskunft über die Arbeitseinkünfte in einem bestimmten Zeitraum. Diese Auskunft wird die Behörde in der Regel nur erhalten, wenn sie dem Arbeitgeber mitteilt, für welche Verwaltungsentscheidung sie die Daten benötigt.

Zu Abs. 1 Nr. 2

Eine Übermittlung kann auch erfolgen, wenn der Empfänger ein **rechtliches Interesse** an der Kenntnis der in Rede stehenden Daten glaubhaft macht und die übermittelnde Stelle keinen Grund zur Annahme hat, dass das **schutzwürdige Interesse des Betroffenen** an der Geheimhaltung überwiegt. Ein rechtliches Interesse ist auf die Durchsetzung von Rechtsansprüchen oder die Abwehr von Forderungen gerichtet. Das rechtliche Interesse ist glaubhaft zu machen. Eine bloße Behauptung reicht dazu nicht aus, notwendig ist vielmehr, dass eine überwiegende Wahrscheinlichkeit für die Richtigkeit der behaupteten Umstände spricht. Ist das rechtliche Interesse zu bejahen, wird in der Regel kein Grund für die Annahme schutzwürdiger Interessen des Betroffenen ersichtlich sein, die der Übermittlung entgegenstehen könnten.

Zu Abs. 1 Nr. 3

Die Übermittlung ist überdies zulässig, wenn sie im öffentlichen Interesse liegt oder ein berechtigtes Interesse des Empfängers an der Kenntnis der Daten besteht und in beiden Fällen ein Widerspruch des Betroffenen gegen die Übermittlung nicht vorliegt. Ein berechtigtes Interesse ist jedes ideelle oder wirtschaftliche Interesse, das mit der Rechtsordnung in Einklang steht. Kurz gesagt: Jedes nicht verbotene Interesse außer der reinen Neugier. Der Betroffene ist in diesen Fällen von einer beabsichtigten Übermittlung zu unterrichten. Widerspricht er der Übermittlung nicht, ist diese zulässig.

Datenschutzfreundlich ist die Regelung der Nr. 3 nicht. Da es um einen Grundrechtseingriff geht, läge eine Vorschrift nahe, die die Rechtssphäre des Betroffenen von vornherein unangetastet lässt und diesen nicht dazu zwingt, erst durch eine eigene Abwehrmaßnahme dem geplanten Rechtseingriff zu begegnen. Überdies kann diese Abwehr unter bestimmten Umständen fehlschlagen. Beispiel: Die Behörde kündigt dem Betroffenen eine Übermittlung an, wenn er dieser nicht bis zu einem bestimmten Zeitpunkt widerspricht. Zur Zeit der Information ist der Betroffene in Urlaub, nach Urlaubsrückkehr ist die Datenübermittlung erfolgt. Eine Vorschrift, die eine Übermittlung in diesen Fällen von der Einwilligung des Betroffenen abhängig machen würde, würde der Bedeutung des Rechts auf informationelle Selbstbestimmung besser entsprechen als die drzeitige Widerspruchslösung.

2. Wie die übrigen Befugnisnormen des NDSG lässt § 13 die Datenübermittlung unter den in der Vorschrift genannten Voraussetzungen zwar zu, verpflichtet die öffentliche Stelle jedoch nicht zu dieser Datenverarbeitung. Die Behörde kann z. B. im Hinblick auf den entstehenden Verwaltungsaufwand eine begehrte Datenübermittlung ohne weiteres ablehnen, auch wenn die rechtlichen Voraussetzungen nach den Vorschriften des NDSG erfüllt sind. Eine entsprechende Verpflichtung zur Datenverarbeitung besteht nur, wenn diese ausdrücklich festgelegt ist.

Zu Abs. 2

3. Der **Empfänger** darf die Daten nur für den Zweck verarbeiten, für den sie ihm übermittelt wurden. Eine unbefugte Nutzung ist unter den Voraussetzungen des § 28 strafbar.

§ 14
Übermittlung an Personen oder Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums

(1) [1]Die Übermittlung personenbezogener Daten an Personen und Stellen in Staaten außerhalb der Europäischen Union und der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sowie an über- und zwischenstaatliche Stellen ist zulässig, soweit die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaften oder einem internationalen Vertrag geregelt ist. [2]Eine Übermittlung an öffentliche Stellen darf auch erfolgen, wenn die Voraussetzungen des § 11 Abs. 1, sowie an andere Empfänger, wenn die Voraussetzungen des § 13 Abs. 1 erfüllt sind und im Empfängerland gleichwertige Datenschutzregelungen gelten. [3]Die Übermittlung nach Satz 2 darf nicht erfolgen, soweit Grund zu der Annahme besteht, dass die Übermittlung einen Verstoß gegen wesentliche Grundsätze des deutschen Rechts, insbesondere gegen Grundrechte, zur Folge haben würde.

(2) Eine Übermittlung ist abweichend von Absatz 1 Satz 2 auch dann zulässig, wenn sie

1. **für die Wahrnehmung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,**
2. **für die Wahrung lebenswichtiger Interessen der Betroffenen erforderlich ist oder**
3. **aus einem Register erfolgt,**

   a) das zur Information der Öffentlichkeit bestimmt ist oder
   b) in das alle Personen, die ein berechtigtes Interesse an der Einsichtnahme haben, Einsicht nehmen können,

soweit der ausländische Empfänger die Voraussetzungen für die Einsichtnahme erfüllt.

Zu Abs. 1 und 2

1. Die EG-Datenschutzrichtlinie verpflichtet die Mitgliedstaaten der Europäischen Union, ein **einheitliches Datenschutzniveau** zu schaffen. Mit Erreichen dieses Ziels sind Übermittlungsbeschränkungen aus Datenschutzgründen gegenüber den Mitgliedstaaten nicht mehr zulässig. Zwar gilt die EG-Datenschutzrichtlinie nur für Verarbeitungen, die in den Anwendungsbereich des Gemeinschaftsrechts fallen, das NDSG erstreckt diese Rechtsfolge darüber hinaus jedoch auf alle Verarbeitungsvorgänge. Dies ist nicht nur im Hinblick auf das Zusammenwachsen der europäischen Rechtsordnungen zu begrüßen, es erleichtert auch die Rechtsanwendung, da eine Prüfung, ob eine bestimmte Übermittlung dem Gemeinschaftsrecht unterliegt oder nicht, entbehrlich wird. Einbezogen in die Regelung sind die übrigen Staaten des

europäischen Wirtschaftsraums (Island, Liechtenstein und Norwegen). Eine Übermittlung an öffentliche oder nicht öffentliche Stellen innerhalb des europäischen Wirtschaftsraums richtet sich nach den gleichen Vorschriften wie eine innerstaatliche Datenübermittlung (§§ 11 und 13).

2. Eine Datenübermittlung in **Länder außerhalb der EU und der übrigen Vertragsstaaten des europäischen Wirtschaftsraums** (Drittländer) darf zunächst vorgenommen werden, wenn bereichsspezifische Regelungen in einem Gesetz, einem Rechtsakt der europäischen Gemeinschaften oder einem internationalen Vertrag dies zulassen. Darüber hinaus darf eine solche Übermittlung erfolgen, wenn die Voraussetzungen der Übermittlungsvorschriften des NDSG (§§ 11, 13) erfüllt sind und gleichwertige Datenschutzregelungen im Empfängerland bestehen. Das NDSG stellt damit höhere Anforderungen an die Übermittlung in Drittländer als die EG-Datenschutzrichtlinie, die lediglich das Vorhandensein eines „angemessenen Schutzniveaus“ im Drittland verlangt (Art. 25 Abs. 2).

3. Gleichwertig sind die Datenschutzregelungen im **Empfängerland**, wenn der Kernbestand der Schutzprinzipien des NDSG dort rechtlich und tatsächlich gewährleistet ist. Dazu gehört insbesondere die Geltung des Zweckbindungsprinzips, das Vorhandensein von Informationsrechten und Kontrollmöglichkeiten sowie Sicherheitsmaßnahmen für die Datenverarbeitung. Für die **Feststellung der Gleichwertigkeit** kommt es nicht darauf an, dass im Drittland Regelungen vorhanden sind, die den Vorschriften des NDSG konkret entsprechen; ein geringerer Datenschutzstandard bei einer bestimmten Verarbeitung kann ausgeglichen werden durch verstärkte Schutzmaßnahmen in anderem Zusammenhang. Auch bei vielfältigen Abweichungen in den Einzelregelungen muss die Gesamtbetrachtung jedoch eine Gleichwertigkeit ergeben. In diesem Zusammenhang stellt Satz 3 klar, dass eine Übermittlung untersagt ist, wenn Grund zur Annahme besteht, dass sie einen Verstoß gegen wesentliche Grundsätze des deutschen Rechts, insbesondere gegen Grundrechte, zur Folge haben würde.

4. Die Daten verarbeitende Stelle wird mit der Beurteilung, ob im Drittland gleichwertige datenschutzrechtliche Regelungen vorhanden sind, in der Regel überfordert sein. Zur Sicherung einer einheitlichen Entscheidungspraxis sind deshalb generelle Festlegungen auf Bundes- oder Landesebene notwendig.

Zur Frage, ob ein Drittstaat ein „angemessenes Schutzniveau“ gewährleistet, wie es Art. 25 Abs. 1 der EG-Datenschutzrichtlinie fordert, trifft die **Europäische Kommission** die notwendigen Feststellungen. Sofern sie zum Ergebnis kommt, dass in bestimmten Staaten ein solches Schutzniveau nicht besteht, darf eine Datenübermittlung dorthin nicht stattfinden. Die positive Feststellung eines solchen Schutzniveaus erlaubt für niedersächsische Stellen die Datenübermittlung jedoch wegen der strikteren Forderung des NDSG nach Gleichwertigkeit der Regelungen noch nicht ohne weiteres.

Fehlen im Drittland gleichwertige Datenschutzregelungen, darf unter den in Abs. 2 genannten Fällen dennoch eine Übermittlung erfolgen. Diese Ausnahmetatbestände gehen auf Art. 26 der EG-Datenschutzrichtlinie zurück.

§ 15
Übermittlung an Stellen öffentlich-rechtlicher Religionsgesellschaften

[1]Die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften ist zulässig, wenn

1. **die Betroffenen eingewilligt haben,**
2. **eine Rechtsvorschrift dies vorsieht,**
3. **sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen,**
4. **offensichtlich ist, dass die Übermittlung im Interesse der Betroffenen liegt und sie einwilligen würden, oder**
5. **sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben**

und sichergestellt ist, dass bei den Empfängern ausreichende Datenschutzmaßnahmen, insbesondere Regelungen zur Zweckbindung, getroffen sind. [2]In den Fällen des Satzes 1 Nr. 5 sind die Betroffenen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten.

Zu § 15

1. § 15 enthält eine besondere Regelung für die Übermittlung personenbezogener Daten an Stellen **öffentlicher Religionsgesellschaften**. Die Übermittlung personenbezogener Daten an privatrechtliche Religionsgesellschaften ist unter den in § 13 genannten Voraussetzungen zulässig. Auch privatrechtlich organisierte Einrichtungen und Werke öffentlich-rechtlicher Religionsgesellschaften gehören nicht zu den in § 15 genannten Stellen; für die Übermittlung von Daten an diese gilt § 13.

2. Die Übermittlung an Stellen öffentlich-rechtlicher Religionsgesellschaften nach § 15 Satz 1 Nrn. 3 bis 5 ist nur zulässig, wenn neben den in der Vorschrift genannten sonstigen Voraussetzungen sichergestellt ist, dass bei den Empfängern ausreichende Datenschutzmaßnahmen getroffen sind. Die **öffentlich-rechtlichen Religionsgesellschaften,** bei denen davon ausgegangen werden kann, dass ausreichende Datenschutzmaßnahmen getroffen sind, werden in den Verwaltungsvorschriften zu § 15 genannt.

Dritter Abschnitt

Rechte der Betroffenen

§ 16
Auskunft, Einsicht in Akten

(1) [1]Betroffenen ist von der Daten verarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. **die zu ihrer Person gespeicherten Daten,**
2. **den Zweck und die Rechtsgrundlage der Speicherung,**
3. **die Herkunft der Daten, die Empfänger von Übermittlungen, in den Fällen des § 6 auch die Auftragnehmer, sowie**
4. **in den Fällen des § 10 a über die Art und Struktur der automatisierten Verarbeitung.**

[2]Dies gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. [3]Für gesperrte Daten, die nur deshalb noch gespeichert sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, gilt die Verpflichtung zur Auskunftserteilung nur, wenn Betroffene ein berechtigtes Interesse an der Erteilung der Auskunft über diese Daten glaubhaft machen.

(2) [1]In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnet werden. [2]Die Daten verarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(3) Sind die Daten in Akten gespeichert, so können Betroffene Auskunft aus Akten oder Akteneinsicht verlangen, soweit sie Angaben machen, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen.

(4) Anträge nach Absatz 1 oder 3 können abgelehnt werden, soweit und solange

1. **die Erfüllung des Auskunfts- oder Einsichtsverlangens die ordnungsgemäße Wahrnehmung der übrigen Aufgaben der datenverarbeitenden Stelle gefährden würde,**
2. **die Auskunft oder Einsicht die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder**
3. **die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen von Dritten geheim zu halten sind.**

(5) [1]Die Ablehnung der Auskunft oder der Akteneinsicht bedarf keiner Begründung, soweit durch die Begründung der Zweck der Ablehnung gefährdet würde. [2]Die Gründe der Ablehnung sind aktenkundig zu machen.

(6) Wird die Auskunft oder die Akteneinsicht abgelehnt, so sind die Betroffenen darauf hinzuweisen, dass sie sich an die Landesbeauftragte oder den Landesbeauftragten wenden können.

(7) Auskunft und Akteneinsicht sind kostenfrei.

Zu Abs. 1

1. Der **Auskunftsanspruch** ist eine Hauptvoraussetzung, um das Recht auf informationelle Selbstbestimmung geltend machen zu können. Hierauf hat bereits das Bundesverfassungsgericht im sog. Volkszählungsurteil hingewiesen („Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich.“ – BVerfGE 65, 1 (46)).

Der Auskunftsanspruch besteht unabhängig von Alter, Nationalität, Wohnsitz und Geschlecht. Er kann von jeder Person geltend gemacht werden, die über die notwendige Einsichts- und Urteilsfähigkeit verfügt.

Der Auskunftsanspruch erstreckt sich über die personenbezogenen Daten des Betroffenen hinaus auch auf den Zweck und die Rechtsgrundlage der Speicherung, die Herkunft der Daten und die Empfänger von Übermittlungen einschließlich der Auftragnehmer bei einer Datenverarbeitung im Auftrag (§ 6).

In den Fällen automatisierter Einzelentscheidungen (§ 16 Abs. 1 Nr. 4) bezieht sich das Auskunftsrecht darüber hinaus auch auf die Art und Struktur der automatisierten Verarbeitung der entsprechenden Daten (vgl. § 10 a Abs. 3). Die Betroffenen müssen erkennen können, in welcher Weise aus ihren Daten eine Bewertung von Persönlichkeitsmerkmalen abgeleitet wird (s. auch Erläuterung zu § 10 a Abs. 3).

Der Anspruch bezieht sich auf den zur Zeit der Antragstellung vorhandenen Datenbestand. Stellt die öffentliche Stelle im Zusammenhang mit dem Auskunftsersuchen fest, dass Daten nicht hätten gespeichert werden dürfen oder zur Aufgabenerfüllung nicht mehr erforderlich sind, darf sie diese Daten nicht ohne weiteres unter Hinweis auf § 17 löschen. Sie muss vielmehr zunächst den Auskunftsanspruch erfüllen, somit dem Betroffenen die Daten mitteilen und ihn auf ihre Löschungsabsicht hinweisen.

Kein Auskunftsrecht besteht für

- personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind (z. B. sog. Log-Dateien).
- Daten, die auf Grund gesetzlicher Aufbewahrungsbestimmungen noch nicht gelöscht werden dürfen und deshalb gesperrt sind, wird nur Auskunft gegeben, wenn die Betroffenen an der Erteilung der Auskunft ein berechtigtes Interesse glaubhaft machen.

Zu Abs. 2

2. Der Auskunftsantrag ist form- und fristlos möglich. Es empfiehlt sich jedoch, ihn schriftlich zu stellen. Um der Behörde ein schnelleres Auffinden der Daten zu ermöglichen, soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnet werden (§ 16 Abs. 2). Die Form der Auskunftserteilung bestimmt die Daten verarbeitende Stelle nach pflichtgemäßem Ermessen. Bei einem mündlichen Antrag muss sie zunächst die Identität des Antragstellers (in der Regel aufgrund von Legimitationspapieren) prüfen und das Ergebnis festhalten. Fernmündliche Auskünfte sind grundsätzlich nicht zu erteilen, weil auch ein Rückruf beim Antragsteller oftmals keine sichere Gewähr bezüglich der Identität des Anrufers ergibt.

Zu Abs. 3

3. Bei einer Datenspeicherung in Akten kann der Betroffene anstelle des Auskunftsrechts auch ein **Akteneinsichtsrecht** geltend machen. Er hat die freie Wahl zwischen beiden Rechten. Bei einem Auskunftsbegehren aus Akten obliegt ihm allerdings eine verstärkte **Mitwirkungspflicht**. Er muss konkrete Hinweise geben (z. B. die handelnde Verwaltungseinheit oder die konkrete Verwaltungsaufgabe benennen), damit die Daten aufgefunden werden können. Einen unangemessenen Aufwand für das Aufsuchen der Daten, der außer Verhältnis zum Informationsinteresse des Betroffenen steht, braucht die Verwaltung nicht zu leisten. In einem solchen Fall kann sie die Akteneinsicht ablehnen.

Den Betroffenen sollte gestattet werden, Auszüge oder Abschriften selbst zu fertigen oder sich Ablichtungen durch die Behörde erteilen zu lassen. Im Gegensatz zu § 25 Abs. 5 SGB X sieht § 16 zwar nicht ausdrücklich ein entsprechendes Recht für den Betroffenen vor, im Hinblick auf eine ermessensfehlerfreie Entscheidung der Behörde sollte dem Begehren des Betroffenen aber entsprochen werden soweit dem keine besonderen Gründe entgegenstehen.

Zu Abs. 4

4. Von der Verpflichtung zur Auskunftserteilung/Akteneinsicht ist keine öffentliche Stelle ausgenommen. Liegt einer der in der Vorschrift genannten drei Ausnahmetatbestände vor, können Auskunft bzw. Akteneinsicht verweigert werden.

Zu Abs. 4 Nr. 1:

Die **ordnungsgemäße Aufgabenwahrnehmung** der Daten verarbeitenden Stelle kann durch die Umstände, aber auch durch den Inhalt der Auskunft gefährdet werden. Ersteres wäre z. B. der Fall, wenn Bürgerinnen und Bürger in einem politisch umstrittenen Verwaltungsverfahren durch gezielte Anfragen in einer derartigen Anzahl Auskunfts- oder Akteneinsichtsbegehren stellen würden, dass die sonstige Verwaltungstätigkeit weitgehend lahmgelegt würde. Bezüglich der Bewertung von Erschwernissen für die Verwaltung ist aber zu beachten, dass das Gesetz die Erteilung von Auskunft/Akteneinsicht in Nr. 1 ausdrücklich als eigene Verwaltungsaufgabe bezeichnet, die neben (nicht etwa erst nach) den übrigen Verwaltungsaufgaben zu sehen ist. Eine stärkere Belastung der Verwaltung durch eine häufigere Wahrnehmung dieser

Rechte stellt deshalb nicht automatisch einen Ablehnungsgrund dar. Der Inhalt der Auskunft/Akteneinsicht kann zu einer Gefährdung der Aufgabenwahrnehmung führen, wenn die öffentliche Stelle durch das Bekanntwerden der Daten (z. B. bei Ermittlungen gegen den Betroffenen) eine Aufgabe nicht mehr sachgerecht erledigen könnte. Außerhalb des Sicherheitsbereichs wird eine Abfrage der eigenen personenbezogenen Daten in der Regel nicht zu einer Gefährdung im Sinne der Nrn. 1 und 2 führen.

Zu Abs. 4 Nr. 2:

Mit der **Gefährdung der öffentlichen Sicherheit** knüpft das Gesetz an das allgemeine Recht der Gefahrenabwehr an (vgl. § 2 Nr. 1 a Nds. SOG). Die öffentliche Sicherheit umfasst nach allgemeiner Auffassung den Schutz vor Schäden, die dem Leben, der Gesundheit, der Ehre, der Freiheit und dem Vermögen des Einzelnen sowie dem Staat, seinen Einrichtungen und seiner Rechtsordnung drohen. Nachteile für das Wohl des Bundes oder eines Landes kommen insbesondere bei einer Gefährdung der inneren oder äußeren Sicherheit in Betracht. In der Verwaltungspraxis haben diese Ablehnungsgründe außerhalb des Bereichs der Gefahrenabwehr, soweit ersichtlich, bisher keine Rolle gespielt.

Zu Abs. 4 Nr. 3:

Geheimhaltungsvorschriften können eine Auskunfts-/Akteneinsichtverweigerung nur begründen, wenn die Geheimhaltungspflicht auch gegenüber dem Betroffenen besteht. Solche Vorschriften sind selten. Als Beispiel kann auf § 61 Abs. 2 Satz 1, Abs. 3 Satz 2 Personenstandsgesetz (PStG) verwiesen werden, wonach im Falle der Adoption, der Nichtehelichkeit oder der Ehelichkeitserklärung Einsicht in Personenstandsbücher erst nach Vollendung des 16. Lebensjahres erteilt wird. Die allgemeine dienstrechtliche Verschwiegenheitspflicht steht einem Auskunfts-/Akteneinsichtsrecht nicht entgegen.

Dass Daten wegen **berechtigter Interessen Dritter** gegenüber dem Betroffenen geheim zu halten sind, ergibt sich insbesondere in Fällen, in denen Informanten einer öffentlichen Stelle Hinweise geben, um diese zu einem Einschreiten zu veranlassen. Beispiel: Ein Bürger teilt der Fahrerlaubnisbehörde mit, dass ein bestimmter Kraftfahrer wegen regelmäßigen Drogengebrauchs zum Führen von Kraftfahrzeugen ungeeignet sei. Will der Betroffene, dem dies bekannt geworden ist, den Namen des Informanten erfahren, stellt sich die Frage, ob die öffentliche Stelle die Auskunft verweigern darf. Diese Frage bedarf einer Interessenabwägung im Einzelfall. Im Allgemeinen wird das Interesse der öffentlichen Stelle, auch künftig sachdienliche Hinweise aus der Bevölkerung zu etwaigen Missständen zu erhalten, um diese abstellen zu können, das Interesse des Betroffenen überwiegen, den Informanten zur Rechenschaft zu ziehen. Liegen jedoch Anhaltspunkte dafür vor, dass der Informant wider besseres Wissen gehandelt hat oder eine unrichtige Sachverhaltsdarstellung in Schädigungsabsicht gegeben hat, kann ein schutzwürdiges Interesse des Informanten nicht mehr angenommen werden.

Zu Abs. 5 und 6

5. Die Ablehnung des Antrags ist zu begründen, es sei denn, dass durch die Begründung selbst der Zweck der Ablehnung gefährdet würde. Auch wenn ausnahmsweise von einer Begründung abgesehen werden kann, müssen die Ablehnungsgründe jedoch aktenkundig gemacht werden. Der Betroffene ist in einem solchen Fall darauf hinzuweisen, dass er sich an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz wenden kann. Dieser oder diesem gegenüber hat die öffentliche Stelle den Sachverhalt zu offenbaren, sodass eine datenschutzrechtliche Prüfung gewährleistet ist. Nach deren Abschluss wird dem Betroffenen mitgeteilt, ob die Ablehnung rechtmäßig war oder nicht. Weitere inhaltliche Informationen können ihm nicht gegeben werden, um den Zweck des Versagungstatbestandes nicht zu unterlaufen.

Der Betroffene hat darüber hinaus die Möglichkeit, im Rahmen eines Widerspruchsverfahrens bzw. eines anschließenden gerichtlichen Verfahrens die Ablehnung überprüfen zu lassen.

Zu Abs. 7

6. Die **Kostenfreiheit** der Auskunft und des Akteneinsichtsrechts schließt nicht aus, dass die Behörde für die Herstellung von Kopien den Ersatz ihrer Aufwendungen in angemessenem Umfang verlangt (vgl. Nr. 1 der Anlage 1.03 zur Allgemeinen Gebührenordnung - AllGO -).

§ 17
Berichtigung, Löschung und Sperrung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) [1]Personenbezogene Daten sind zu löschen, wenn

1. **ihre Speicherung unzulässig ist oder**
2. **ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.**

[2]In den Fällen des Satzes 1 Nr. 2 tritt an die Stelle der Löschung die Abgabe an das zuständige Archiv, soweit dies in den entsprechenden Rechtsvorschriften vorgesehen ist. [3]Sind personenbezogene Daten in Akten gespeichert, so ist die Löschung nach Satz 1 Nr. 2 durchzuführen, wenn die gesamte Akte nach Maßgabe der entsprechenden Rechts- oder Verwaltungsvorschriften zur Aufgabenerfüllung nicht mehr erforderlich ist. [4]Werden durch die weitere Speicherung nach Satz 3 schutzwürdige Belange der Betroffenen erheblich beeinträchtigt, so sind die entsprechenden Daten zu sperren.

(3) [1]Personenbezogene Daten sind zu sperren,

1. **solange und soweit ihre Richtigkeit von den Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,**
2. **wenn die Betroffenen anstelle der Löschung unzulässig gespeicherter Daten die Sperrung verlangen oder die weitere Speicherung im Interesse der Betroffenen geboten ist, oder**
3. **solange sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen.**

[2]Gesperrte Daten sind mit einem Sperrvermerk zu versehen; in automatisierten Verfahren ist die Sperrung durch zusätzliche technische Maßnahmen zu gewährleisten. [3]Gesperrte Daten dürfen nicht mehr weiter verarbeitet werden, es sei denn, dass dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder Dritter liegenden Gründen unerlässlich ist oder die Betroffenen eingewilligt haben. [4]Die Gründe für die Verarbeitung gesperrter Daten sind aufzuzeichnen.

(4) [1]Sind Daten nach den Absätzen 1 bis 3 berichtigt, gesperrt oder gelöscht worden, so sind die Personen oder Stellen unverzüglich zu unterrichten, denen die Daten übermittelt worden sind. [2]Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden.

Zu Abs. 1

1. Unrichtig können nur Tatsachenbehauptungen sein, weil nur bei ihnen ein Wahrheitsbeweis möglich ist. Werturteile können deshalb grundsätzlich nicht berichtigt werden, es sei denn, dass sie auf einer falschen Tatsachengrundlage beruhen. Beispiel: Die Bezeichnung eines Bürgers als „unzuverlässig“ in einem bestimmten Lebenszusammenhang ist als Werturteil, dagegen als Tatsachenbehauptung dann anzusehen, wenn es sich auf bestimmte Verhaltensweisen des Betroffenen stützt.. Die Aussage ist unrichtig, wenn die betreffenden Verhaltensweisen in Wahrheit nicht vorgelegen haben.

Die Art der Berichtigung schreibt das Gesetz nicht vor. Sie bleibt der Daten verarbeitenden Stelle überlassen. Unrichtige Daten können gelöscht und durch die richtigen Daten ersetzt werden. Das zu berichtigende Datum kann auch als unrichtig gekennzeichnet und das richtige hinzugefügt werden. Ein mehrfach in Akten enthaltenes unrichtiges Datum muss nicht an jeder Stelle berichtigt werden, die Berichtigung kann vielmehr durch einen vorangestellten Vermerk erfolgen.

Zu Abs. 2

2. Löschen (§ 3 Abs. 2 S. 2 Nr. 6) ist das Unkenntlichmachen von Daten in einer Weise, dass diese nicht wieder zugänglich gemacht werden können. Der Löschungsvorgang muss irreversibel sein. Auf die DIN 32757-1: 1995-01 zur Vernichtung von Informationsträgern und die DIN 33858: 1993-04 zum Löschen von schutzbedürftigen Daten auf flexiblen Datenträgern (Disketten, Bänder) wird verwiesen. Eine DIN für die Löschung von Daten auf Fest- und Wechselplatten gibt es derzeit noch nicht. Die Daten solcher Medien sollten vor ihrer Vernichtung mittels Zerkleinerung oder Stoffumwandlung durch starke Magneten gelöscht werden.

Nach Satz 1 Nr. 1 sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Dieser Fall ist insbesondere dann gegeben, wenn Daten ohne ausreichende Ermächtigungsgrundlage oder zur Aufgabenerfüllung nicht erforderliche Daten erhoben worden sind oder eine unzulässige Datenerhebung bei Dritten vorgelegen hat. Nach Satz 1 Nr. 2 sind Daten zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Mit dem Wegfall der Erforderlichkeit entfällt auch die Befugnis zur Datenverarbeitung.

3. Bei einer Datenverarbeitung in Akten sind Daten, deren Speicherung unzulässig ist (Satz 1 Nr. 1) unverzüglich zu löschen; Daten, deren Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist (Satz 1 Nr. 2) dagegen erst dann, wenn die gesamte Akte nach den einschlägigen Aufbewahrungsvorschriften zur Aufgabenerfüllung nicht mehr erforderlich ist.

4. Vor der Löschung ist jeweils zu prüfen, ob die Daten

- zu sperren sind. Dies ist bei einem Verlangen des Betroffenen oder seinem dahingehenden Interesse (Abs. 3 Satz 1 Nr. 2) oder bei gesetzlichen Aufbewahrungsfristen (Abs. 3 Satz 1 Nr. 3) der Fall.
- als schutzwürdiges Archivgut vom Archiv übernommen werden. Nach den archivrechtlichen Bestimmungen sind nicht mehr erforderliche Daten dem Archiv anzu-

bieten (§§ 3, 7 NArchG). Entscheidet dieses, dass die Daten aufbewahrungswürdig sind, werden sie vom Archiv übernommen. Eine Löschung unterbleibt. Nicht archivwürdige Daten werden dagegen gelöscht.

Bei unzulässig gespeicherten Daten (Abs. 2 Satz 1 Nr. 1) kommt eine Abgabe an das Archiv nicht in Betracht (§ 3 Abs. 3 NArchG). Daneben gibt es weitere Rechtsvorschriften, nach denen bestimmte Daten unverzüglich von der jeweils zuständigen Dienststelle zu löschen sind (u. a. § 17 Abs. 3 NDiszG, Nr. 3 der VV-Kor).

Zu Abs. 3

5. Sperren (§ 3 Abs. 2 S. 2 Nr. 5) ist das Kennzeichnen von Daten, um ihre weitere Verarbeitung einzuschränken. Um dies zu erreichen, müssen sie von anderen Daten deutlich unterschieden werden; sie sind deshalb mit einem Sperrvermerk zu versehen.

Eine Sperrung hat in den in Abs. 2 Satz 4 und Abs. 3 genannten Fällen zu erfolgen. Eine Sperrung im Interesse des Betroffenen (Abs. 3 S. 1 Nr. 2) ist insbesondere geboten, wenn der Betroffene auf Grund der Datenspeicherung einen Schadensersatzanspruch geltend machen will und die an sich vorgesehene Löschung seiner Daten die Durchsetzung dieses Anspruchs beeinträchtigen oder vereiteln könnte.

Personenbezogene Daten, die noch nicht gelöscht werden dürfen, weil die in der Aktenordnungen bzw. in den Aktenplänen genannten Aufbewahrungsfristen nicht abgelaufen sind (vgl. VV NDSG, Nr. 18.1 zu § 17, Erläuterungen S. 158), deren Kenntnis für die Aufgabenerfüllung jedoch nicht mehr erforderlich ist, sind zu sperren.

Die Sperrung von Daten führt zu einem grundsätzlichen Verbot der weiteren Datenverarbeitung. Eine Weiterverarbeitung ist nur zulässig bei Einwilligung des Betroffenen oder wenn dies zur Behebung einer Beweisnot oder aus sonstigen Gründen im überwiegenden Interesse der speichernden Stelle oder Dritter unerlässlich ist. An diese Ausnahmen sind hohe Anforderungen zu stellen. Das überwiegende Interesse muss im Rahmen einer Rechtsgüterabwägung ermittelt werden. Es muss von erheblich höherem Gewicht sein als das Grundrecht des Betroffenen auf informationelle Selbstbestimmung.

Die Gründe für die Weiterverarbeitung gesperrter Daten sind zu dokumentieren.

Zu Abs. 4

6. Wenn Daten, die später berichtigt, gelöscht oder gesperrt worden sind, anderen Personen oder Stellen übermittelt wurden, erfordert es der Grundrechtsschutz des Betroffenen, die empfangende Stelle von den durchgeführten Korrekturen zu unterrichten, damit sie ebenfalls entsprechende Maßnahmen treffen kann. Auch diese Unterrichtung muss die Daten verarbeitende Stelle belegen können.

Die Unterrichtung kann in den in Satz 2 aufgelisteten Fällen unterbleiben. Auf Nr. 18.2 der VV NDSG zu § 17 wird verwiesen.

§ 17 a
Widerspruchsrecht

[1]Betroffene haben gegenüber der Daten verarbeitenden Stelle das Recht, der Verarbeitung der sie betreffenden Daten aus schutzwürdigen persönlichen Gründen zu widersprechen. [2]Soweit diese Gründe überwiegen, ist die Verarbeitung der Daten unzulässig. [3]Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Zu § 17 a

Die Vorschrift geht auf Art. 14 der EG-Datenschutzrichtlinie zurück. Sie räumt dem Betroffenen das Recht ein, einer an sich rechtmäßigen Verarbeitung seiner Daten aus besonderen persönlichen Gründen zu widersprechen. Das **Widerspruchsrecht**, das nicht mit dem Widerspruch in verwaltungsgerichtlichen Vorverfahren nach §§ 69 ff. VwGO verwechselt werden darf, zwingt die öffentliche Stelle, die beabsichtigte Datenverarbeitung im Hinblick auf die vom Betroffenen geltend gemachte besondere persönliche Situation zu überprüfen. Die Vorschrift will damit besonderen Sachverhaltskonstellationen im Einzelfall gerecht werden.

Ergibt die Prüfung, dass die geltend gemachten persönlichen Gründe des Betroffenen das Interesse der öffentliche Stelle an der Datenverarbeitung überwiegen, ist die Verarbeitung unzulässig. Ggf. sind die in Rede stehenden Daten nach § 17 Abs. 2 Nr. 1 zu löschen.

Das Widerspruchsrecht ist weder an eine bestimmte Form noch an eine Frist gebunden. Aus Zweckmäßigkeitsgründen empfiehlt sich allerdings eine schriftliche Geltendmachung des Anspruchs. Bis zur Entscheidung über den Widerspruch muss die fragliche Datenverarbeitung zurückgestellt werden, damit die Erfüllung des Anspruchs nicht vereitelt wird.

Gibt die Daten verarbeitende Stelle dem Antrag nicht statt, so handelt es sich bei dieser Ablehnung um einen Verwaltungsakt, gegen den die üblichen Rechtsmittel gegeben sind.

Wenn eine Rechtsvorschrift zur Verarbeitung der Daten verpflichtet, entfällt das Widerspruchsrecht. Mit einer solchen Regelung hat der Gesetzgeber eindeutig zum Ausdruck gebracht, dass die Daten zu verarbeiten sind.

Die praktische Bedeutung der Vorschrift dürfte im Hinblick auf ihren **Ausnahmecharakter** begrenzt sein. Als denkbarer Anwendungsfall lässt sich anführen, dass ein Betroffener geltend macht, ein Vorgang, der seine höchstpersönlichen Daten zum Gegenstand habe (z. B. eine Untersuchung durch den Amtsarzt), dürfe nicht vom zuständigen Bediensteten bearbeitet werden, weil dieser zu seinem Bekanntenkreis gehöre, ohne dass er bereits nach dem Verwaltungsverfahrensrecht von der Mitwirkung an dem Vorgang ausgeschlossen sei. Ergibt die Prüfung durch die öffentliche Stelle, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen zu bejahen ist, muss die Bearbeitung durch einen anderen Bediensteten erfolgen.

§ 18
Schadensersatz

(1) [1]Wird den Betroffenen durch eine nach datenschutzrechtlichen Vorschriften unzulässige Verarbeitung ihrer personenbezogenen Daten ein Schaden zugefügt, so sind ihnen die Träger der Daten verarbeitenden Stellen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet; im Fall einer nicht automatisierten Verarbeitung besteht die Ersatzpflicht nicht, wenn die Daten verarbeitende Stelle nachweist, dass die Unzulässigkeit nicht von ihr zu vertreten ist. [2]Bei einer schweren Verletzung des Persönlichkeitsrechts kann auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangt werden. [3]Ersatzpflichtige haften gegenüber jeder betroffenen Person für jedes schädigende Ereignis bis zu einem Betrag von 250 000 Euro. Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(2) Auf ein Mitverschulden der Betroffenen ist § 254 und auf die Verjährung des Schadensersatzanspruchs § 199 Abs. 3 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

Zu § 18

1. Die Ausgestaltung der Vorschrift orientiert sich am Ablauf und den Risiken der Verarbeitung personenbezogener Daten. Sie trägt den spezifischen Bedingungen der Verwendung personenbezogener Daten Rechnung, indem sie eine **Gefährdungshaftung** ohne Rücksicht darauf statuiert, ob die Verarbeitung manuell oder automatisiert erfolgt. Dies entspricht der EG-Datenschutzrichtlinie. Sonstige Schadensersatzansprüche bleiben von der Regelung unberührt. Neben vertraglichen Schadensersatzansprüchen kommen bei **hoheitlicher Tätigkeit** vor allem die Ansprüche aus § 839 BGB i.V.m. Art. 34 GG und bei **fiskalischer Tätigkeit** gemäß §§ 823, 31, 89 bzw. 831 BGB in Betracht.

Zu Abs. 1

2. Die Regelung sieht in Satz 1 Halbsatz 1 eine Gefährdungshaftung vor. Diese ist allein abhängig von einer unzulässigen Verarbeitung personenbezogener Daten und einem dadurch adäquat-kausal eingetretenen Schaden. Die Frage des Verschuldens der Daten verarbeitenden Stelle ist grundsätzlich ohne Bedeutung. Derjenige, der durch die Verarbeitung personenbezogener Daten eine Gefahr für das Recht auf informationelle Selbstbestimmung hervorruft, soll auch ohne eigenes Verschulden für etwaige Schäden einstehen müssen. Dem Betroffenen obliegt der Nachweis der rechtswidrigen Verarbeitung und der Schadensverursachung. Für die nicht automatisierte Verarbeitung sieht Halbsatz 2 eine **Beweislastumkehr** vor. Kann die für die Datenverarbeitung verantwortliche Stelle bei der nicht automatisierten Verarbeitung von Daten nachweisen, dass die Unzulässigkeit der Datenverarbeitung nicht von ihr zu vertreten ist, so entfällt eine Ersatzpflicht. Auf diese Weise trägt der Gesetzgeber

dem unterschiedlichen Risiko- und Gefährdungspotential von automatisierter und manueller Datenverarbeitung Rechnung. Dieses ist bei der automatisierten Verarbeitung höher zu bewerten und rechtfertigt einen strengeren Haftungsmaßstab.

3. Anspruchsberechtigt sind Personen, die durch die unzulässige Verarbeitung ihrer Daten geschädigt worden sind. Dritte können einen Schaden, der dadurch entstanden ist, dass sie z. B. aufwändige Vorkehrungen treffen mussten, um eine Verwendung der ihnen von der Meldebehörde überlassenen, jedoch unzulässig verarbeiteten Daten zu verhindern, nicht ersetzt verlangen. Stets muss es sich um Daten handeln, die dem Anwendungsbereich des NDSG unterfallen. Für Schäden, die durch die in § 2 Abs. 3 und 4 genannten Wettbewerbsunternehmen in Ausübung ihrer wirtschaftlichen Tätigkeit oder durch öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen verursacht werden, gelten dagegen die Schadensersatzregelungen der §§ 7 und 8 BDSG.

4. Die Haftung setzt eine **„unzulässige“ Verarbeitung** voraus. Unzulässig ist jede Verarbeitung, die gegen Vorschriften über den Datenschutz verstößt. Dies gilt z. B. auch, wenn die Daten verarbeitende Stelle einer Pflicht zur Benachrichtigung des Betroffenen nicht nachkommt (vgl. § 13 Abs. 1 Satz 2) oder es versäumt, unrichtige Daten zu sperren bzw. zu löschen (§ 17 Abs. 2 und 3). Die Gefährdungshaftung tritt dagegen nicht ein bei einer Verarbeitung unrichtiger Daten, etwa bei falschen Angaben über die Einkommensverhältnisse.

Ersetzt werden in erster Linie **materielle Schäden**, also im Regelfall Vermögensschäden. Diese müssen adäquat-kausal auf der unzulässigen Verarbeitung der Daten beruhen, d.h. die rechtswidrige Verarbeitung muss die Möglichkeit des Schadens generell nicht unerheblich erhöht haben. Die Möglichkeit des Schadenseintritts darf nicht so entfernt sein, dass sie nach der Lebenserfahrung vernünftigerweise nicht in Betracht gezogen werden kann. Nach Satz 2 wird auch der sog. immaterielle Schaden ersetzt, soweit eine schwere Verletzung des Persönlichkeitsrechts eingetreten ist. Wann eine solche vorliegt, definiert das Gesetz nicht. Maßgeblich ist im Einzelfall der objektive Umfang der Beeinträchtigung. Je nachhaltiger die Diskriminierung von Betroffenen etwa durch eine unzulässige Übermittlung von Daten ist und je schärfer sich in ihrem privaten oder beruflichen Bereich und erst recht in der Öffentlichkeit ein Bild ihrer Person abzeichnet, das sie in ihrer Handlungs- und Entscheidungsfreiheit beschränkt, desto zwingender erscheint ein finanzieller Ausgleich. Immaterielle Schäden sind unabhängig davon auszugleichen, ob die Betroffenen einen Anspruch auf Ersatz materieller Schäden haben.

5. Die Haftung ist nach Satz 3 gegenüber jedem Betroffenen „für jedes schädigende Ereignis“ auf 250 000 Euro begrenzt. Auf die Art des Schadens kommt es nicht an. Entscheidend ist allein die Höhe des gesamten Schadens. Sobald sie die gesetzlich festgelegte Deckungsgrenze übersteigt, kann der darüber hinausgehende Betrag, jedenfalls nach § 18, nicht mehr geltend gemacht werden. Die in Satz 4 für den Fall der Haftung mehrerer Träger vorgesehene gesamtschuldnerische Haftung entspricht § 840 Abs. 1 BGB. Den Umfang der Haftung regelt das BGB in §§ 421 ff. Den Betroffenen steht es daher frei, entweder einen Träger für den gesamten jeweils

entstandenen Schaden in Anspruch zu nehmen oder von jedem einen bestimmten Teilbetrag zu verlangen (§ 421 Satz 1 BGB). Gleicht einer der Träger den Schaden aus, werden auch die übrigen Schuldner von ihrer Ersatzpflicht befreit (§ 422 Abs. 1 Satz 1 BGB). Die Schadensersatzleistung begründet im Innenverhältnis einen Regressanspruch gegenüber den für den Schaden mitverantwortlichen Trägern. Der Schadensersatzanspruch ist im Übrigen zu gleichen Teilen von allen Trägern zu tragen, es sei denn, sie haben besondere Abmachungen für den Fall einer Schadensersatzleistung getroffen (§ 426 Abs. 1 Satz 1 BGB). Die Betroffenen können ihre Ersatzansprüche vor den Zivilgerichten geltend machen (§ 40 Abs. 2 Satz 1 VwGO).

Zu Abs. 2

6. Durch den Hinweis auf § 254 BGB wird klargestellt, dass der Schadensersatzanspruch ggf. entfällt, wenn z. B. der Betroffene die Unrichtigkeit der Daten selbst verschuldet hat, weil er falsche Angaben gemacht oder gegenüber einer ihm bekannten unrichtigen Speicherung keinen Berichtigungsanspruch geltend gemacht hat. Die Regelung des § 254 BGB ist lediglich entsprechend anwendbar, weil ein Mitverschulden begrifflich ein die Haftung begründendes Verschulden voraussetzt. Daran fehlt es bei der Gefährdungshaftung. Durch die uneingeschränkte Verweisung auf § 254 BGB kommt auch § 254 Abs. 2 Satz 2 BGB zum Tragen, nach dem sich der geschädigte Betroffene ein Mitverschulden seiner gesetzlichen Vertreter und seiner Erfüllungsgehilfen zurechnen lassen muss.

7. Der Anspruch verjährt auf Grund der Anwendung des § 199 Abs. 3 BGB. In Betracht kommt sowohl eine Verjährung nach § 199 Abs. 3 Nr. 1 als auch nach Nr. 2 BGB. Maßgeblich ist nach § 199 Abs. 3 S. 2 BGB die früher endende Frist. Der Schadensersatzanspruch ist auch bei reinen Persönlichkeitsrechtsverletzungen nach Absatz 1 Satz 2 übertragbar und vererblich.

§ 19
Anrufung der Landesbeauftragten oder des Landesbeauftragten

(1) [1]Jede Person, die meint, durch die Verarbeitung ihrer personenbezogenen Daten in ihren Rechten durch eine Stelle verletzt worden zu sein, die der Kontrolle nach den Vorschriften dieses Gesetzes unterliegt, kann sich an die Landesbeauftragte oder den Landesbeauftragten wenden. [2]Keine Person darf deswegen benachteiligt werden.

(2) [1]Die Bediensteten der Behörden und sonstigen öffentlichen Stellen, auf die dieses Gesetz Anwendung findet, dürfen sich unbeschadet ihres Rechts nach Absatz 1 in allen Angelegenheiten des Datenschutzes jederzeit an die Landesbeauftragte oder den Landesbeauftragten wenden. [2]Der Einhaltung des Dienstweges bedarf es nicht, wenn die Bedienstete oder der Bedienstete auf einen Verstoß gegen datenschutzrechtliche Vorschriften oder auf die Gefahr hingewiesen hat, dass eine Person in unzulässiger Weise in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt wird, und diesem Hinweis binnen angemessener Frist nicht abgeholfen worden ist. [3]Im Übrigen bleiben die dienstrechtlichen Pflichten der Bediensteten unberührt.

Zu § 19

1. Zu den Rechten des Betroffenen gehört die Anrufung der oder des Landesbeauftragten für den Datenschutz. Das **Anrufungsrecht** entspricht dem **Petitionsrecht** nach Art. 17 GG. Es besteht selbstständig neben jenem sowie neben dem Recht, sich an die Gerichte zu wenden. Mit der oder dem Landesbeauftragten wird eine Institution zur Verfügung gestellt, die das Vertrauen des Betroffenen darauf stärkt, dass er seine Rechte auch gegenüber einer durch fortschreitende Technisierung und zunehmende Komplexität undurchschaubar gewordenen Verwaltung durchsetzen kann.

Zu Abs. 1

2. Berechtigt, sich an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz zu wenden, ist nach Satz 1 jede Person, die durch die Verarbeitung von personenbezogenen Daten in ihren Rechten verletzt sein kann. Das ist der Betroffene, zu dessen Schutz das NDSG erlassen worden ist. Ein Dritter, dessen Daten nicht verarbeitet werden, der aber von einer unrechtmäßigen Datenverarbeitung erfährt, kann sich zwar an die Landesbeauftragte oder den Landesbeauftragten wenden und ihr oder ihm dies mitteilen, es handelt sich aber nicht um eine Anrufung nach § 19. Entsprechendes gilt für juristische Personen, die nicht Betroffene sein können, weil das NDSG nur Daten natürlicher Personen schützt. Das Anrufungsrecht gilt auch für Bedienstete von Behörden und sonstigen öffentlichen Stellen, wenn sie meinen, in eigenen Rechten verletzt zu sein; im Übrigen siehe Erläuterungen zu Abs. 2.

3. Das Recht zur Anrufung der oder des Landesbeauftragten für den Datenschutz besteht nur insoweit, als der Betroffene tatsächlich oder vermeintlich bei der Verarbeitung von Daten in seinen Rechten verletzt worden ist. Stets muss es sich um Verhal-

tensweisen handeln, die sich auf die Verwendung und Sicherung personenbezogener Daten oder die Ausübung der Rechte des Betroffenen beziehen. Sonstige Rechte und Interessen, die keinen Bezug zum Datenschutz haben, genügen nicht. Das Recht, dessen Verletzung behauptet wird, kann im NDSG gründen, aber auch in jeder anderen Rechtsnorm mit Datenschutzcharakter. Die oder der Datenschutzbeauftragte kann auch wegen einer nur drohenden Rechtsverletzung angerufen werden, z. B. wenn eine Behörde die Erhebung bestimmter Daten des Betroffenen beabsichtigt. Er braucht nicht erst den Vollzug der Maßnahme abzuwarten.

4. Das Anrufungsrecht ist nicht an die Voraussetzung geknüpft, dass eine Rechtsverletzung tatsächlich vorliegt. Es reicht aus, wenn der Betroffene „meint“, in seinen Rechten verletzt worden zu sein. Er muss angeben, aufgrund welchen Sachverhalts er sich verletzt fühlt. Einer bestimmten **Form** bedarf es nicht. Die Anrufung kann daher schriftlich oder mündlich, auch fernmündlich erfolgen, zweckmäßig ist es jedoch, die Schriftform zu wählen. An irgendwelche **Fristen** ist die Anrufung nicht gebunden. Ist der Sachverhalt unvollständig dargestellt oder ist nicht eindeutig zu erkennen, inwiefern ein Recht des Betroffenen verletzt sein soll, hat die oder der Landesbeauftragte für den Datenschutz dem Betroffenen mitzuteilen, dass die Bearbeitung nur möglich ist, wenn er seine Angaben entsprechend ergänzt. Werden diese Bedingungen nicht erfüllt, braucht die Eingabe nicht weiter bearbeitet zu werden. Sie kann aber zum Anlass für ein Tätigwerden von Amts wegen genommen werden. Stets muss es sich um eine öffentliche Stelle handeln, die der Kontrolle durch die oder den Landesbeauftragten für den Datenschutz gemäß § 22 Abs. 2 Satz 1 und 2 unterliegt. Das sind die Behörden und sonstigen öffentlichen Stellen des Landes. Eingaben, welche die Verarbeitung personenbezogener Daten durch den Landtag, die Gerichte und den Landesrechnungshof betreffen, darf die oder der Datenschutzbeauftragte nur nachgehen, soweit diese in Verwaltungsangelegenheiten tätig geworden sind. Entscheidungen, die z. B. ein Gericht in richterlicher Unabhängigkeit getroffen hat, unterliegen nicht der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten.

5. Die Betroffenen haben einen Anspruch darauf, dass ihre Eingaben erledigt werden. Dazu sind die Eingaben entgegen zu nehmen und zu bearbeiten. Die Betroffenen sind über das Ergebnis in geeigneter Weise zu unterrichten. Eine detaillierte Begründung ist nicht vorgeschrieben. Soweit zur Aufklärung des Sachverhalts erforderlich, hat die oder der Landesbeauftragte für den Datenschutz im Rahmen der Kompetenzen (§ 22 Abs. 1 und 6) und Befugnisse (§ 22 Abs. 4) ergänzende **Ermittlungen** durchzuführen. Diese Verpflichtung wird in der Regel dadurch erfüllt, dass den betroffenen Behörden oder öffentlichen Stellen Gelegenheit zur Äußerung gegeben wird. Stellt die oder der Landesbeauftragte eine Rechtsverletzung fest, muss angegeben werden, durch welchen Vorgang welche Rechtsverletzung eingetreten ist. Die Betroffenen haben aber keinen Anspruch, dass ihren Begehren entsprochen oder eine Beanstandung ausgesprochen wird. Erfolgt die Anrufung ersichtlich in beleidigender Absicht oder aus sonstigen sachfremden Erwägungen, ist die oder der Datenschutzbeauftragte berechtigt, die Bearbeitung abzulehnen. Die abschließende **Unterrichtung des Betroffenen** ist kein Verwaltungsakt. Es wird kein Einzelfall

geregelt, die Unterrichtung ist auch nicht auf unmittelbare Rechtswirkung nach außen gerichtet. Daher scheidet eine Anfechtungsklage aus. Es besteht auch sonst kein gerichtlicher Rechtsbehelf gegen die Mitteilung der oder des Landesbeauftragten für den Datenschutz, da die Klagebefugnis wegen fehlender Möglichkeit einer Rechtsverletzung nicht gegeben ist (vgl. § 42 Abs. 2 VwGO).

Zu Abs. 2

6. Die Bediensteten der Behörden und sonstigen öffentlichen Stellen im Sinne von § 2 dürfen nach Satz 1 unabhängig davon, ob sie durch die Verarbeitung personenbezogener Daten in eigenen Rechten betroffen sind, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz anrufen. Denkbar ist dies nicht nur bei einer drohenden Beeinträchtigung von Rechten Dritter, sondern in „allen Angelegenheiten“ des Datenschutzes, soweit eine öffentliche Stelle Daten verarbeitet. Die Bediensteten haben dabei grundsätzlich den Dienstweg einzuhalten, es sei denn, die Voraussetzungen des Satzes 2 erlauben eine unmittelbare Anrufung der Landesbeauftragten oder des Landesbeauftragten. Unabhängig hiervon können Bedienstete jederzeit die behördlichen Datenschutzbeauftragten ihrer öffentlichen Stelle ansprechen (vgl. § 8 a Anm. 12).

§ 20
Verzicht auf Rechte der Betroffenen

Die in diesem Abschnitt genannten Rechte können auch durch die Einwilligung der Betroffenen nicht im Voraus ausgeschlossen oder beschränkt werden.

Zu § 20

Die Vorschrift stellt klar, dass die Rechte der Betroffenen nach § 16 (Auskunft, Akteneinsichtsrecht), § 17 (Berichtigung, Löschung, Sperrung), § 17 a (Widerspruchsrecht), § 18 (Schadensersatz) und § 19 (Anrufung der oder des Landesbeauftragten) unabdingbar sind. Ein vorheriger Verzicht auf diese Rechte ist nicht möglich, selbst wenn die Betroffenen dies ausdrücklich, auch schriftlich, erklären. Allerdings haben die Betroffenen selbstverständlich die Möglichkeit, von den Rechten keinen Gebrauch zu machen.

Vierter Abschnitt

Landesbeauftragte oder Landesbeauftragter für den Datenschutz

§ 21
Rechtsstellung der Landesbeauftragten oder des Landesbeauftragten

(1) [1]Die Landesbeauftragte oder der Landesbeauftragte soll die Befähigung zum Richteramt haben. [2]Sie oder er wird nach der Wahl durch den Landtag auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen. [3]Die Wiederwahl und die Berufung für eine weitere Amtszeit sind zulässig. [4]Das Amt ist im Übrigen bis zum Eintritt der Nachfolge weiterzuführen. [5]Die Landesbeauftragte oder der Landesbeauftragte kann außer auf Antrag nur entlassen werden, wenn der Pflicht nach Satz 4 nicht nachgekommen wird oder wenn Gründe vorliegen, die bei einem Richterverhältnis auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

(2) [1]Für die Landesbeauftragte oder den Landesbeauftragten gilt keine Altersgrenze. [2]§ 37 des Niedersächsischen Beamtengesetzes ist nicht anzuwenden.

(3) [1]Die Landesbeauftragte oder der Landesbeauftragte ist Leiterin oder Leiter einer von der Landesregierung unabhängigen obersten Landesbehörde mit Sitz in Hannover. [2]Soweit dienstrechtliche Befugnisse der Landesregierung zustehen, werden Stellen auf Vorschlag der Landesbeauftragten oder des Landesbeauftragten besetzt. [3]Die Bediensteten können ohne ihre Zustimmung nur im Einvernehmen mit der Landesbeauftragten oder dem Landesbeauftragten versetzt, abgeordnet oder umgesetzt werden.

Zu § 21

1. Nach der Rechtsprechung des Bundesverfassungsgerichts aus dem Jahre 1983 (s. sog. „Volkszählungsurteil“, BVerfGE 65, 1, 46) ist „die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung“. In der **Niedersächsischen Verfassung** (NV) ist in Artikel 62 die Funktion der oder des Landesbeauftragten für den Datenschutz als eine institutionalisierte Fremdkontrolle mit folgenden Regelungen verfassungsrechtlich abgesichert:

„Artikel 62 NV

Landesbeauftragte oder Landesbeauftragter für den Datenschutz

(1) [1]Die oder der Landesbeauftragte für den Datenschutz kontrolliert, dass die öffentliche Verwaltung bei dem Umgang mit personenbezogenen Daten Gesetz und Recht einhält. [2]Sie oder er berichtet über ihre oder seine Tätigkeit und deren Ergebnisse dem Landtag.

(2) [1]Der Landtag wählt auf Vorschlag der Landesregierung die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz mit einer Mehrheit von zwei Dritteln der anwesenden Mitglieder des Landtages, mindestens jedoch der Mehr-

heit seiner Mitglieder. [2]Die oder der Landesbeauftragte für den Datenschutz wird von der Landesregierung ernannt und entlassen.

(3) [1]Die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz ist unabhängig und nur an Gesetz und Recht gebunden. [2]Artikel 38 Abs. 1 und Artikel 56 Abs. 1 finden auf sie oder ihn keine Anwendung.

(4) [1]Das Nähere bestimmt ein Gesetz. [2]Dieses Gesetz kann personalrechtliche Entscheidungen, welche Bedienstete der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz betreffen, von deren oder dessen Mitwirkung abhängig machen. [3]Der Landesbeauftragten oder dem Landesbeauftragten für den Datenschutz kann durch Gesetz die Aufgabe übertragen werden, die Durchführung des Datenschutzes bei der Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen zu kontrollieren “

Die Wahl der oder des Landesbeauftragten durch den Landtag und die Festlegungen zu ihrer oder seiner Unabhängigkeit belegen die **Sonderstellung dieser Funktion**, die sich dadurch manifestiert, dass die Landesbeauftragte oder der Landesbeauftragten für den Datenschutz ein Verfassungsorgan ist.

Die Vorgabe der qualifizierten Mehrheit in Artikel 62 Abs. 2 NV soll dabei sicherstellen, dass die oder der Landesbeauftragte für den Datenschutz von dem Vertrauen einer breiten Mehrheit der Abgeordneten getragen wird. Dies ist zugleich eine unverzichtbare Voraussetzung für eine effektive unabhängige Amtsführung.

2. In den §§ 21 bis 23 sind auf Grund dieser Vorgaben die Einzelheiten zur Rechtsstellung, zu den Aufgaben und zu den Befugnissen der oder des Landesbeauftragten für den Datenschutz geregelt.

3. Zur **Sicherung der Unabhängigkeit** ist dabei in § 21 Abs. 1 Satz 5 festgelegt, dass die Landesbeauftragte oder der Landesbeauftragte während der achtjährigen, als Beamtenverhältnis auf Zeit ausgestalteten Amtszeit - außer auf Antrag - nur bei einer Verletzung ihrer oder seiner Pflichten aus Abs. 1 Satz 4 oder aus Gründen, die auch bei einem Richter auf Lebenszeit eine Entlassung aus dem Dienst rechtfertigen würden, ihres oder seines Amtes enthoben werden kann.

Die neue Rechtsstellung der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz ist an die Rechtsstellung des Landesrechnungshofs angeglichen werden. Die Vorschrift ist angelehnt an § 5 Abs. 2 Satz 1 des Gesetzes über den Niedersächsischen Landesrechnungshof (LRHG).

Als von der Landesregierung unabhängige oberste Landesbehörde ist die oder der Landesbeauftragte auch oberste Dienstbehörde nach § 3 Abs. 1 Niedersächsisches Beamtengesetz.

Die bisherige Geschäftsstelle der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz ist seit dem 08. Juli 2011 eine unabhängige oberste Landesbehörde, mit der Landesbeauftragten oder dem Landesbeauftragten als Behördenleitung.

§ 21 a
Disziplinarverfahren

(1) In Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten gelten die Vorschriften des Niedersächsischen Disziplinargesetzes nach Maßgabe der folgenden Absätze.

(2) [1]Für Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten ist der Niedersächsische Dienstgerichtshof für Richter (Dienstgerichtshof) zuständig. [2]Entscheidungen des Dienstgerichtshofs im Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten werden mit der Verkündung oder der sie ersetzenden Zustellung rechtskräftig.[3]Der Dienstgerichtshof entscheidet auf Antrag der Präsidentin oder des Präsidenten des Landtages.

(3) [1]Der Verweis ist als Disziplinarmaßnahme ausgeschlossen. [2]Über die vorläufige Dienstenthebung und die Einbehaltung von Dienstbezügen sowie über die Aufhebung dieser Maßnahmen entscheidet auf Antrag der Präsidentin oder des Präsidenten des Landtages der Dienstgerichtshof durch Beschluss.

(4) [1]Die nicht ständigen Mitglieder des Dienstgerichtshofs müssen der Verwaltungsgerichtsbarkeit angehören. [2]Auf die Besetzung des Dienstgerichtshofs finden im Übrigen die §§ 81 bis 83, 86 Abs. 2 Satz 1 und Abs. 4 und 5 sowie die §§ 87 und 88 des Niedersächsischen Richtergesetzes entsprechende Anwendung.

Zu § 21a

1. Aufgrund der Stellung der oder des Landesbeauftragten für den Datenschutz als oberste Landesbehörde ist für Disziplinarverfahren gegen die Landesbeauftragte oder den Landesbeauftragten als Leiterin oder Leiter dieser Behörde eine von § 5 Abs. 1 Niedersächsisches Disziplinargesetz (NDiszG) abweichende Zuständigkeit geregelt. Ähnlich wie beim Landesrechungshof (vgl. § 7 LRHG) gibt es nur ein gerichtliches Disziplinarverfahren. Zuständig ist wie beim Landesrechnungshof der Niedersächsische Dienstgerichtshof für Richter. Die nicht ständigen Mitglieder des Dienstgerichtshofs sollen aufgrund der Sachnähe der Verwaltungsgerichtsbarkeit angehören. Das Antragsrecht ist § 7 Abs. 3 LRHG nachgebildet. Der Gerichtshof wird nicht von Amts wegen tätig, sondern es bedarf stets eines Antrages (Klageerhebung oder Antrag im Eilverfahren) der Präsidentin oder des Präsidenten des Landtages.

2. In Absatz 2 Satz 1 wird der Verweis als Disziplinarmaßnahme ausgeschlossen, da für diese Maßnahme ein gerichtliches Verfahren nicht geeignet erscheint. Absatz 2 Satz 2 enthält eine § 96 Abs. 1 des Niedersächsischen Richtergesetzes (NRiG) entsprechende Vorschrift.

Die Verweisung auf das NRiG in Absatz 4 stellt klar, dass die darin enthaltenen Regelungen über die Besetzung des Gerichtshofs entsprechend anzuwenden sind, soweit im NDSG keine abweichenden Regelungen getroffen wurden. Abweichend geregelt ist in § 21 a, dass die nicht ständigen Beisitzer Richterinnen oder Richter der

Verwaltungsgerichtsbarkeit sein müssen. Für das Verfahren vor dem Dienstgerichtshof gelten im Übrigen die Vorschriften für das gerichtliche Disziplinarverfahren im NDiszG entsprechend. Ihrem Sinn nach nicht anwendbar sind z. B. die Vorschriften, die ein behördliches Disziplinarverfahren voraussetzen.

Für die der oder dem Landesbeauftragten für den Datenschutz nachgeordneten Beamtinnen und Beamten gilt das NDiszG unverändert, d. h. die oder der Landesbeauftragte für den Datenschutz ist in diesen Fällen zuständige Disziplinarbehörde nach § 5 NDiszG.

§ 21 b
Übertragung von Aufgaben

[1]Überträgt die Landesbeauftragte oder der Landesbeauftragte Aufgaben der Personalverwaltung ganz oder teilweise auf eine andere Behörde, so dürfen personenbezogene Daten aus der Personalakte auch ohne Einwilligung der oder des Betroffenen an diese Behörde übermittelt und von ihr verarbeitet werden, soweit dies für die Erfüllung der übertragenen Aufgabe erforderlich ist.

Zu § 21b

1. Die Landesbeauftragte oder der Landesbeauftragte kann Aufgaben der Personalverwaltung durch eine andere öffentliche Stelle im Auftrag und im Namen der Landesbeauftragten oder des Landesbeauftragten wahrnehmen zu lassen. Die Regelung ist eine über § 92 Abs. 2 NBG hinausgehende Rechtsgrundlage für die Verarbeitung von Personalaktendaten der Beschäftigten der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz (s. § 4 Abs. 1 Nr. 1 i. V. m. § 2 Abs. 6 NDSG).

2. Organisatorische Aufgaben (sog. „Querschnittsaufgaben“), wie z. B. Poststelle, Botendienst und Beschaffung sowie Aufgaben der Haushaltsbewirtschaftung, können im Wege eines Auftrags der Landesbeauftragten oder des Landesbeauftragten von einer anderen Stelle wahrgenommen werden, ohne dass es dazu einer gesetzlichen Regelung bedarf.

§ 22
Aufgaben, Rechte und Pflichten der Landesbeauftragten oder des Landesbeauftragten

(1) [1]Die Landesbeauftragte oder der Landesbeauftragte kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen. [2]Der Landtag, die Gerichte und der Landesrechnungshof unterliegen dieser Kontrolle aber nur, soweit sie in Verwaltungsangelegenheiten tätig werden. [3]Außerdem kann die Landesbeauftragte oder der Landesbeauftragte den Landtag, die Landesregierung, die übrigen Behörden und sonstigen öffentlichen Stellen über Verbesserungen des Datenschutzes beraten. [4]Die Landesbeauftragte oder der Landesbeauftragte ist bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften anzuhören, die Regelungen zum Recht auf informationelle Selbstbestimmung zum Gegenstand haben.

(2) Die Landesbeauftragte oder der Landesbeauftragte ist rechtzeitig über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme zu unterrichten.

(3) [1]Die Landesbeauftragte oder der Landesbeauftragte legt dem Landtag jeweils für zwei Kalenderjahre einen Tätigkeitsbericht vor. [2]Die Landesregierung nimmt hierzu gegenüber dem Landtag innerhalb von sechs Monaten Stellung. [3] Die Landesbeauftragte oder der Landesbeauftragte unterrichtet den Landtag und die Öffentlichkeit auch über wesentliche Entwicklungen des Datenschutzes. [4]Auf Ersuchen des Landtages, seines zuständigen Ausschusses oder der Landesregierung hat die Landesbeauftragte oder der Landesbeauftragte ferner Angelegenheiten von besonderer datenschutzrechtlicher Bedeutung zu untersuchen und über die Ergebnisse zu berichten. [5]Die Landesbeauftragte oder der Landesbeauftragte hat in bedeutsamen Fällen alsbald dem Landtag schriftlich oder in den Sitzungen seiner Ausschüsse mündlich zu berichten. [6]Auf Ersuchen des Landtages oder seines zuständigen Ausschusses hat die Landesbeauftragte oder der Landesbeauftragte auch in sonstigen Fällen über einzelne Vorgänge aus ihrem oder seinem Tätigkeitsbereich zu berichten und auf Ersuchen dazu Akten vorzulegen. [7]Die Landesbeauftragte oder der Landesbeauftragte braucht Ersuchen nach Satz 6 nicht zu entsprechen, soweit dadurch ihre oder seine Funktionsfähigkeit wesentlich beeinträchtigt würde. [8]Schriftliche Äußerungen gegenüber dem Landtag sind gleichzeitig der Landesregierung vorzulegen.

(4) [1]Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten bei der Erfüllung der Aufgaben zu unterstützen. [2]Dazu haben sie insbesondere

1. Auskunft zu erteilen sowie Einsicht in alle Unterlagen zu gewähren, die die Landesbeauftragte oder der Landesbeauftragte zur Erfüllung der Aufgaben für erforderlich hält,
2. die in Nummer 1 genannten Unterlagen auf Verlangen innerhalb einer bestimmten Frist zu übersenden,
3. jederzeit Zutritt in alle Diensträume zu gewähren.

[3]Die oberste Landesbehörde entscheidet, ob der Landesbeauftragten oder dem Landesbeauftragten personenbezogene Daten einer betroffenen Person zu offenbaren sind, wenn dieser Vertraulichkeit besonders zugesichert worden ist.

(5) Beschreibungen nach § 8 sind der Landesbeauftragten oder dem Landesbeauftragten zu übersenden, wenn die Verarbeitungen zur Erfüllung

1. der Aufgaben nach dem Niedersächsischen Verfassungsschutzgesetz oder
2. polizeilicher Aufgaben nach dem Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung

erfolgen.

(6) [1]Die Landesbeauftragte oder der Landesbeauftragte ist auch Aufsichtsbehörde im Sinne des § 38 des Bundesdatenschutzgesetzes für die Kontrolle der Durchführung des Datenschutzes bei der Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen. [2]Absatz 3 Sätze 1, 3 und 5 bis 7 gelten entsprechend.

Zu § 22

Zu Abs. 1 und 2

1. Die **Kontrolltätigkeit** der oder des Landesbeauftragten erfasst den gesamten Bereich der öffentlichen Verwaltung des Landes, der kommunalen Gebietskörperschaften und anderer Stellen der mittelbaren Landesverwaltung. Sie erstreckt sich gemäß § 24 Abs. 6 i. V. m. Abs. 2 BDSG auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, z. B. nach § 203 StGB oder § 30 Abgabenordnung (Steuergeheimnis). Handelt es sich um personenbezogene Daten, für die dem Betroffenen die Vertraulichkeit besonders zugesichert worden ist, entscheidet die oberste Landesbehörde, ob die Daten gegenüber der oder dem Landesbeauftragten zu offenbaren sind (Abs. 4 Satz 3). Bei personenbezogenen Daten in Akten über die Sicherheitsüberprüfung kann der Betroffene der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten widersprechen (§ 24 Abs. 2 Satz 4 i. V. m. Abs. 6 BDSG).

2. Gegenüber dem Landtag und dem Landesrechnungshof sowie gegenüber den Gerichten (nicht aber gegenüber den Staatsanwaltschaften) greift die Kontrolle der oder des Landesbeauftragten wegen deren besonderer Stellung und Unabhängigkeit allerdings nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Gleichwohl

haben auch diese Stellen natürlich das materielle Datenschutzrecht einzuhalten. Der Landtag hat sich bei der Wahrnehmung seiner parlamentarischen Aufgaben in der Datenschutzordnung (vgl. § 2 Abs. 2) der Kontrolle einer aus Abgeordneten gebildeten Datenschutzkommission unterworfen. Bei den Gerichten wäre es sachgerechter und in der Praxis auch klarer abgrenzbar, wenn zur Beschreibung des Kontrollbereiches nicht an die Wahrnehmung von Verwaltungstätigkeiten, sondern an die unmittelbar der Rechtsprechung dienende Tätigkeit angeknüpft würde; hierdurch wäre klargestellt, dass zum Beispiel die Einhaltung der bei allen Tätigkeiten zur Texterfassung und Bearbeitung von Urteilen zu beachtenden Maßnahmen der Datensicherung von der oder dem Landesbeauftragten kontrolliert werden könnten.

3. In der Praxis besteht die Kontrolltätigkeit des Landesbeauftragten nicht nur in der nachträglichen und nachsorgenden Überprüfung von Vorgängen und Vorfällen in der Verwaltung, sie erstreckt sich daneben - anknüpfend an den allgemeinen **Beratungsauftrag** in Abs. 1 Satz 3 - zunehmend auf eine vorsorgende Information und Aufklärung über datenschutzgerechte Lösungen sowie auf die aktive Mitgestaltung im Vorfeld der Entwicklung und bei der Auswahl von Verfahren der automatisierten Verarbeitung und der rechtlichen Begleitregelungen. Dabei bilden vor allem die nunmehr auch gesetzlich verankerten Prinzipien der Datenvermeidung und der Datensparsamkeit (vgl. § 7 Abs. 4) wichtige Orientierungspunkte.

Diese werden ergänzt durch die Regelungen zur frühzeitigen Unterrichtung und Einbindung der oder des Landesbeauftragten für Datenschutz bei Planungen zum Aufbau automatisierter Informationssysteme (Abs. 2) und bei der Ausarbeitung von einschlägigen Rechts- und Verwaltungsvorschriften (Abs. 1 Satz 4) sowie durch die Unterstützungspflichten der Behörden und sonstigen öffentlichen Stellen gegenüber der oder dem Landesbeauftragten (Abs. 4) nachdrücklich gestützt.

Zu Abs. 3

4. Der alle zwei Jahre zu erstattende **Tätigkeitsbericht** ist das wichtigste Instrument, um den Landtag (und die Öffentlichkeit) über datenschutzrechtlich bedeutsame Entwicklungen zu unterrichten. Der Bericht gewinnt zunehmend Bedeutung für die notwendige frühzeitige Darstellung von Zukunftsentwicklungen, insbesondere im Bereich der Informations- und Kommunikationstechnologien und dem daraus abzuleitenden datenschutzpolitischen Handlungsbedarf. Durch den auf Anregung des Landesbeauftragten eingefügten Satz 3 wird unterstrichen, dass die oder der Landesbeauftragte das Recht und die Pflicht hat, den Landtag und die Öffentlichkeit über bedeutsame Entwicklungen auf dem Gebiet des Datenschutzes auch unabhängig von der Vorlage des Tätigkeitsberichtes zu informieren. In der Praxis wird diese **Informationspflicht** – außer durch eine intensive Öffentlichkeits- und Pressearbeit – vor allem durch die Herausgabe von Orientierungshilfen und Handlungsanleitungen, durch ein breites Informations- und Beratungsangebot im Internet (**www.lfd.niedersachsen.de** sowie **www.datenschutz.de**), durch die Einrichtung von Diskussionsforen und elektronisch unterstützten Netzwerken mit den behördlichen und betrieblichen Datenschutzbeauftragten sowie durch eine umfangreiche Beratungs-, Vortrags- und Fortbildungstätigkeit aller Mitarbeiterinnen und Mitarbeiter

der Geschäftsstelle ausgefüllt. Ein wichtiges Ziel dabei ist auch, den Bürgerinnen und Bürgern Informationen und konkrete Hilfestellungen für einen wirkungsvollen Datenselbstschutz an die Hand zu geben.

Zu Abs. 5

5. Beschreibungen für automatisierte Verarbeitungen nach § 8 Abs. 1 sind der oder dem Landesbeauftragten für Datenschutz gemäß Absatz 5 nur noch dann vorzulegen, wenn es sich um Verarbeitungen im Bereich des Verfassungsschutzes oder der Polizei auf der Grundlage des Nds. SOG handelt. Im Übrigen führt jede öffentliche Stelle diese Beschreibungen selbst und hat diese gemäß § 8 a Abs. 2 Satz 4 in einer Übersicht den jeweiligen behördlichen Datenschutzbeauftragten und auf Anfrage den Bürgerinnen und Bürgern zugänglich zu machen.

Zu Abs. 6

6. Die Aufgaben der Aufsichtsbehörde für die Datenverarbeitung im nicht öffentlichen Bereich nach § 38 Abs. 6 BDSG sind dem Landesbeauftragten 1992 durch Beschluss der Niedersächsischen Landesregierung übertragen worden. Dies ist insofern sinnvoll, weil so die hier vorhandenen datenschutzrechtlichen Fachkenntnisse auch für die Wahrnehmung der Aufsichtsaufgaben gegenüber den nicht öffentlichen Stellen, also etwa gegenüber der Wirtschaft, den Verbänden und Vereinen, genutzt und dadurch erhebliche Synergieeffekte erzielt werden können.

6. In seinem Urteil vom 09. März 2010 in der Rechtssache C-518/07 hat der Europäische Gerichtshof festgestellt, dass die staatliche Aufsicht, der die für die Überwachung der Verarbeitung personenbezogener Daten im nicht öffentlichen Bereich zuständigen Kontrollstellen in Deutschland unterworfen sind, nicht mit dem Unabhängigkeitserfordernis des Artikel 28 Abs. 1 Unterabs. 2 der RL 95/46/EG vereinbar sei.

Durch die Neufassung des bisherigen dritten Satzes wird geregelt, dass für die Tätigkeit als Aufsichtsbehörde nach § 38 BDSG nicht nur ein Tätigkeitsbericht nach Absatz 3 vorgelegt werden muss, sondern auch die Unterrichtungs- und Berichtspflichten an den Landtag gelten. Hierdurch soll der Verlust an materieller demokratischer Legitimation, der durch die Streichung der Fachaufsicht entsteht, wenigstens teilweise aufgewogen werden.

§ 23
Beanstandungen durch die Landesbeauftragte oder den Landesbeauftragten

(1) [1]Stellt die Landesbeauftragte oder der Landesbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen fest, so ist dies

1. **bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,**
2. **bei den Gemeinden, Landkreisen und den sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem vertretungsberechtigten Organ**

mit der Aufforderung zu beanstanden, innerhalb einer bestimmten Frist Stellung zu nehmen. [2]In den Fällen des Satzes 1 Nr. 2 ist gleichzeitig auch die zuständige Aufsichtsbehörde zu unterrichten.

(2) [1]Die Stellungnahme soll auch die Maßnahmen darstellen, die der Beanstandung abhelfen sollen. [2]Die in Absatz 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme zu.

(3) Die Landesbeauftragte oder der Landesbeauftragte kann insbesondere dann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt oder die Beseitigung der Mängel sichergestellt ist.

Zu § 23

1. Werden Verstöße gegen datenschutzrechtliche Vorschriften festgestellt, finden in aller Regel mit der betreffenden Stelle zunächst Gespräche statt, in denen versucht wird, datenschutzgerechtes Verhalten bzw. eine Beseitigung der Mängel durchzusetzen. Nur dann, wenn es sich um Verstöße oder Mängel von erheblichem Gewicht handelt oder datenschutzgerechtes Verhalten abgelehnt wird, wird von dem Mittel der förmlichen **Beanstandung** Gebrauch gemacht. Nach Absatz 1 ist die Beanstandung bei Stellen der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde, bei Stellen der kommunalen Gebietskörperschaften oder anderen Stellen der mittelbaren Landesverwaltung gegenüber dem vertretungsberechtigten Organ – mit gleichzeitiger Unterrichtung der zuständigen Aufsichtsbehörde – auszusprechen. Die Beanstandung wird mit der Aufforderung verbunden, innerhalb einer bestimmten Frist unter Bezeichnung der ergriffenen Abhilfemaßnahmen Stellung zu nehmen. Von dem Mittel der förmlichen Beanstandung wird in der Praxis des Landesbeauftragten nur sehr sparsam und in aller Regel erst dann Gebrauch gemacht, wenn die Rückkehr zu datenschutzgerechtem Verhalten beharrlich verweigert wird.

2. Beanstandungen der oder des Landesbeauftragten gegenüber Stellen der öffentlichen Verwaltung sind **keine Verwaltungsakte** oder sonstige Eingriffe in eine Rechtsposition der Daten verarbeitenden Stelle; sie können daher auch nicht vor dem Verwaltungsgericht angefochten werden.

3. Neben der Beanstandung besteht immer die Möglichkeit, Verstöße oder datenschutzwidriges Verhalten im **Tätigkeitsbericht** anzusprechen und dadurch eine Stellungnahme der Landesregierung gegenüber dem Parlament sowie eine politische Diskussion im Landtag herbeizuführen. Diese Möglichkeit wird insbesondere dann ins Auge zu fassen sein, wenn die zu der förmlichen Beanstandung abgegebene Stellungnahme einen festgestellten Verstoß gegen datenschutzrechtliche Vorschriften abstreitet oder in anderer Weise erkennen lässt, dass ein datenschutzgerechtes Vorgehen oder Verhalten in Zukunft nicht sichergestellt ist. In besonders schwerwiegenden Fällen besteht außerdem die Möglichkeit, dem Landtag außerhalb des Tätigkeitsberichts gemäß § 22 Abs. 3 Satz 5 gesondert schriftlich oder in einer Ausschusssitzung mündlich zu berichten. Hiervon musste bisher noch nicht Gebrauch gemacht werden.

4. Soweit die oder der Landesbeauftragte als Kontrollinstanz **im nicht öffentlichen Bereich** tätig wird, richten sich ihre oder seine Aufsichtsmittel nach § 38 BDSG.

§ 24
Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Die beamtenrechtlichen Vorschriften über die Führung von Personalakten gemäß § 50 des Beamtenstatusgesetzes und §§ 88 bis 95 des Niedersächsischen Beamtengesetzes sind für alle nicht beamteten Beschäftigten einer öffentlichen Stelle entsprechend anzuwenden, soweit tarifvertraglich nichts anderes geregelt ist.

(2) [1]Werden Feststellungen über die Eignung einer Bewerberin oder eines Bewerbers für ein Dienstverhältnis durch ärztliche oder psychologische Untersuchungen oder Tests getroffen, so darf die Einstellungsbehörde von der untersuchenden Person oder Stelle in der Regel nur das Ergebnis der Eignungsuntersuchung und solche Feststellungen anfordern, die die gesundheitliche Eignung beeinträchtigen könne (Risikofaktoren). [2]Weitere personenbezogene Daten darf sie nur anfordern, wenn sie die Bewerberin oder den Bewerber zuvor schriftlich über die Gründe dafür unterrichtet hat. [3]Die Weiterverarbeitung der übermittelten und gespeicherten Daten ist nur mit schriftlicher Einwilligung der Bewerberin oder des Bewerbers zulässig.

Zu § 24

1. Die Ursprungsregelung wurde 1993 bei der grundlegenden Überarbeitung des NDSG im Vorgriff auf eine landesrechtliche Umsetzung der Regelungen des damals geltenden Beamtenrechtsrahmengesetzes in das Gesetz aufgenommen. Mit Wirkung vom 31. Dezember 1997 wurde die Regelung gestrichen, da das NBG seinerzeit vergleichbare Regelungen enthielt, die für nicht beamtete Beschäftigte für anwendbar erklärt worden waren (§ 261 Abs. 1 Nr. 2 i. V. m. §§ 101 bis 101h NBG a. F.). Mit Artikel 1 des Gesetzes vom 25. März 2009 (Nds. GVBl. S. 72) wurde das NBG grundlegend neugefasst und in diesem Zuge § 261 NBG wieder gestrichen.

Zu Abs. 1

2. Mit der Wiederaufnahme des § 24 NDSG durch Artikel 1 des Gesetzes zur Änderung des Datenschutzgesetzes und zur Änderung kommunal- und brandschutzrechtlicher Regelungen vom 12. Dezember 2012 (Nds. GVBl. S. 589) sind die sich zwischenzeitlich für den Bereich der nicht beamteten Beschäftigten ergebenen Regelungslücken bei der Verarbeitung von Personaldaten zu Zwecken der Personalplanung und des Personaleinsatzes aufgehoben worden. Die neue Regelung stellt den Gleichklang der Vorschriften für beamtete und nicht beamtete Beschäftigte her.
3. Die Vorschrift hat gegenüber den übrigen Bestimmungen des NDSG einen bereichsspezifischen Charakter, da sie abweichend von den allgemeinen Vorschriften des Gesetzes Besonderheiten des Dienst- und Arbeitsverhältnisses regelt.

Zu Abs. 2

4. Die Vorschriften regeln Besonderheiten des **Bewerbungsverfahrens**. Daten, die bei ärztlichen oder psychologischen Untersuchungen und Tests erhoben worden sind, dürfen nur in dem genannten Rahmen weiterverarbeitet werden. Der Arbeitgeber darf von der untersuchenden Stelle grundsätzlich nur das Ergebnis der Eignungsuntersuchung (geeignet/nicht geeignet) und dabei eventuell festgestellte Risikofaktoren, die einen dienstlichen Einsatz in Frage stellen, anfordern. Fordert er darüber hinaus die Übermittlung weiterer personenbezogener Daten, muss er die Gründe für diese Anforderung dokumentieren und die Bewerber darüber vorab schriftlich unterrichten. Ihnen soll damit die Möglichkeit gegeben werden, unter diesen Umständen ihre Bewerbung zurückzuziehen.

Die Weiterverarbeitung der Daten, wie z. B. die Speicherung für ein weiteres Bewerbungsverfahren, bedarf der schriftlichen Einwilligung der Betroffenen (s. § 4 Abs. 2 NDSG).

§ 25
Verarbeitung personenbezogener Daten für Forschungsvorhaben

(1) Für die Verarbeitung personenbezogener Daten zur Durchführung von wissenschaftlichen Forschungsvorhaben sind die §§ 9 bis 15 nach Maßgabe der Absätze 2 bis 5 und 7 anzuwenden.

(2) Für wissenschaftliche Forschungsvorhaben dürfen personenbezogene Daten, die für andere Zwecke oder für ein anderes Forschungsvorhaben erhoben oder gespeichert worden sind, verarbeitet werden, wenn

1. **die Betroffenen eingewilligt haben,**
2. **eine Rechtsvorschrift dies vorsieht oder**
3. **Art und Verarbeitung der Daten darauf schließen lassen, dass ein schutzwürdiges Interesse der Betroffenen der Verarbeitung der Daten für das Forschungsvorhaben nicht entgegensteht oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der Betroffenen erheblich überwiegt. Das Ergebnis der Abwägung und seine Begründung sind aufzuzeichnen. Über die Verarbeitung ist die Datenschutzbeauftragte oder der Datenschutzbeauftragte nach § 8 a zu unterrichten.**

(3) Die für ein Forschungsvorhaben gespeicherten oder übermittelten Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.

(4) Sobald der Stand des Forschungsvorhabens es gestattet, sind die Merkmale, mit deren Hilfe ein Bezug auf eine bestimmte natürliche Person hergestellt werden kann, gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck dies gestattet.

(5) Im Rahmen von wissenschaftlichen Forschungsvorhaben dürfen personenbezogene Daten nur veröffentlicht werden, wenn

1. **die Betroffenen eingewilligt haben oder**
2. **dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.**

(6) Die Einwilligung der Betroffenen bedarf nicht der Schriftform, wenn hierdurch das Forschungsvorhaben erheblich beeinträchtigt würde.

(7) [1]Eine Übermittlung personenbezogener Daten an Empfänger, auf die dieses Gesetz keine Anwendung findet, ist nach Maßgabe des Absatzes 2 zulässig, wenn sich die Empfänger verpflichten, die Daten nur für das von ihnen zu bezeichnende Forschungsvorhaben und nach Maßgabe der Absätze 3 bis 5 zu

verarbeiten. [2]Die Übermittlung ist der Landesbeauftragten oder dem Landesbeauftragten rechtzeitig vorher anzuzeigen.

Zu § 25

1. § 25 regelt als allgemeine "**Forschungsklausel**" die Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke durch öffentliche Stellen, die Forschung betreiben, sowie die Übermittlung von öffentlichen Stellen an Forschende. Sowohl die **Freiheit der Forschung** (Art. 5 Abs. 3 Satz 1 GG) wie auch das Recht auf informationelle Selbstbestimmung haben Verfassungsrang. Mit § 25 wird ein Ausgleich zwischen den beiden Rechtsgütern und den sich widersprechenden Interessen geschaffen.

2. Zahlreiche Forschungsprojekte kommen ohne jeden Abstrich an der wissenschaftlichen Zielsetzung **ohne personenbezogene Daten** aus. Bei der Übermittlung schon anonymisierter Daten ist § 25 nicht anwendbar. Die Forschenden sollten daher prüfen, ob überhaupt ein Rückgriff auf Personendaten und damit eine Anwendung von § 25 erforderlich ist.

3. Da die mit dem Begriff der wissenschaftlichen Forschung angesprochenen Sachverhalte sehr unterschiedlich sind und § 25 nur allgemeine Grundsätze zur Auflösung des Spannungsverhältnisses zwischen Forschung und Selbstbestimmung aufzeigen kann, bleiben ergänzende oder modifizierende **Datenschutzregelungen** in den jeweiligen Fachgesetzen erforderlich. Dies gilt insbesondere für den Bereich besonderer Berufsgeheimnisse. Teilweise gibt es bereits solche bereichsspezifischen Regelungen. So enthält § 75 SGB X eine besondere Forschungsregelung für die Übermittlung von Sozialdaten. Soweit sich Datenerhebungs- und Datenübermittlungsregelungen aus bereichsspezifischen Gesetzen ergeben, die keine Aussage zur Nutzung für Forschungszwecke enthalten, kann auf die Rechtsgrundsätze des § 25 ergänzend zurückgegriffen werden.

4. Wenn eine öffentliche niedersächsische Stelle Forschungsvorhaben durchführt, bei denen eine **Datenerhebung in anderen Bundesländern** erfolgt, hat die Forschungsstelle zunächst die Zulässigkeit der Datenerhebung nach niedersächsischem Recht zu prüfen. Ob die Datenübermittlung durch Stellen des Bundes oder anderer Länder zulässig ist, richtet sich nach den für diese geltenden Datenschutzbestimmungen und ist von den übermittelnden Stellen in eigener Zuständigkeit zu prüfen; die Datenübermittlung durch Private richtet sich nach den Regeln des BDSG.

5. Führt eine öffentliche Stelle ein Forschungsvorhaben **mit eigenen Daten** durch, so ist diese Verarbeitung zulässig, wenn auch die Forschung zum Aufgabenbereich der jeweiligen Stelle gehört (§ 10 Abs. 1). Dies ist z. B. in Universitätskliniken bei Forschungsprojekten durch die behandelnden Ärzte der Fall. Die Weitergabe dieser Daten an Doktorandinnen und Doktoranden oder sonstige Angehörige der jeweiligen Stelle, die nicht an der Behandlung beteiligt sind, ist eine nach § 25 i. V. m. § 11 Abs. 4 zulässige Offenbarung. § 10 Abs. 3 ist anzuwenden, wenn Ausbildungszwecke verfolgt werden.

6. Sollen bei einem Forschungsprojekt **Daten von Verstorbenen** erhoben oder sonst wie verarbeitet werden, so ist § 25 nicht anwendbar. Das NDSG schützt nur Daten natürlicher lebender Personen (§ 3 Abs. 1). Der Umgang mit diesen Daten kann dennoch unzulässig sein, z. B. wenn die Daten der Verstorbenen unter ein besonderes Berufsgeheimnis fallen (z. B. Arztgeheimnis, vgl. § 203 StGB) und keine Offenbarungsbefugnis besteht. In diesen Fällen kann eine entsprechende Anwendung der Grundsätze von § 25 in Frage kommen. Zu beachten ist in diesen Fällen oft auch das **Archivrecht**.

7. Für die Annahme eines Forschungsvorhabens muss der **Forschungszweck hinreichend bestimmt** festgelegt werden. Eine allgemeine wissenschaftliche Zweckbestimmung reicht nicht aus. Werden bei einem Forschungsprojekt Folgevorhaben durchgeführt, so handelt es sich um eigenständige Vorhaben.

Zu Abs. 1

8. Für die Verarbeitung von personenbezogenen Daten für Forschungsvorhaben gelten die **allgemeinen Regelungen der §§ 9 bis 15**. Sie werden durch § 25 Abs. 2 bis 5 und 7 nur modifiziert und bleiben im Übrigen anwendbar. In jedem Fall bedarf es der Prüfung, ob die Datenverarbeitung für den bestimmten wissenschaftlichen Zweck im konkreten Umfang tatsächlich **erforderlich** ist. Für die Erhebung von Forschungsdaten bedeutet dies, dass deren Zulässigkeit nach § 9 zu beurteilen ist (z. B. Vorrang der Erhebung bei den Betroffenen).

Zu Abs. 2

9. Will eine Forschungsstelle auf bereits vorhandene Daten zurückgreifen, die für andere Zwecke oder auch für ein anderes Forschungsvorhaben erhoben oder gespeichert worden sind, so liegt darin eine **Zweckänderung** dieser Daten. Der Hauptanwendungsfall ist die Erhebung personenbezogener Daten durch die forschende Einrichtung bei öffentlichen Stellen, die diese Daten für Verwaltungszwecke gespeichert haben. Sie ist nach § 25 Abs. 2 zulässig bei Einwilligung der Betroffenen (Nr. 1), beim Vorliegen einer entsprechenden Rechtsvorschrift (Nr. 2; dazu gehören auch Satzungen von Selbstverwaltungskörperschaften wie den Hochschulen) oder wenn die Belange der Betroffenen hinter dem Interesse am Forschungsvorhaben zurücktreten müssen (Nr. 3). Nach § 25 Abs. 2 Nr. 3 dürfen vorhandene Daten abweichend von ihrer ursprünglichen Zweckbestimmung ohne Einwilligung der Betroffenen verarbeitet werden, wenn Art und Verarbeitung der Daten darauf schließen lassen, dass ein schutzwürdiges Interesse der Betroffenen der Verarbeitung der Daten für das Forschungsvorhaben nicht entgegensteht (1. Alternative) oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der Betroffenen erheblich überwiegt (2. Alternative).

10. Es kann regelmäßig nur im konkreten Fall festgestellt werden, ob **schutzwürdigen Interessen** der Betroffenen einer Verarbeitung für Forschungszwecke entgegenstehen (Abs. 2 Nr. 3, 1. Alternative). Schutzwürdige Interessen stehen zumeist dann nicht entgegen, wenn Daten aus allgemein zugänglichen Quellen entnommen werden. Entsprechendes kann angenommen werden, wenn relativ "unsensible"

Daten (ohne Bezug zur Privat- und Intimsphäre und ohne Bezug zum Sozialverhalten) sofort anonymisiert und danach erst wissenschaftlich ausgewertet werden.

11. Das **öffentliche Interesse** wird durch die Hochschule, den Hochschullehrer oder den sonstigen Forschenden als Inhaber des Forschungsrechts festgestellt. Wenn allerdings das Forschungsvorhaben von einer Privatperson oder einer anderen nicht öffentlichen Stelle oder einer öffentlichen Stelle, die nicht in den Anwendungsbereich des NDSG fällt (z. B. eine Stelle des Bundes oder eines anderen Bundeslandes) durchgeführt wird, ist die Abwägung von der übermittelnden Stelle durchzuführen (VV 23.2 zu § 25). Der Begriff „öffentliches Interesse“ ist nicht nur im Sinne eines staatlichen oder Verwaltungsinteresses zu verstehen. Die Annahme des öffentlichen Interesses orientiert sich an der gesellschaftlichen oder wissenschaftlichen Bedeutung des untersuchten Gegenstands. Ist zu erwarten, dass mit Hilfe der Forschungsergebnisse besondere im Gemeinwohl liegende Maßnahmen ermöglicht werden (z. B. Vermeidung von Straftaten, Bekämpfung von Krankheiten, Beseitigung einer Umweltgefahr), so spricht dies in besonderem Maße für ein öffentliches Interesse. Das öffentliche Interesse kann durch Gesetze (z. B. Gesundheits- oder Umweltgesetze) oder durch ministerielle Entscheidungen bekräftigt werden.

12. Für **entgegenstehende Betroffeneninteressen** sprechen u. a. folgende Umstände: die Sensibilität der erhobenen Daten (z. B. gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, arbeitsrechtliche Verhältnisse, Daten mit Diskriminierungsrisiko, z. B. genetische Disposition, HIV-Infektion, Schwangerschaftsabbruch, psychische Erkrankung), der Umfang des erhobenen Datensatzes und der damit erfassten Lebensbereiche (Familie, Beruf, Freizeitverhalten, Gesundheit), das zeitlich weite Zurückliegen eines privaten Sachverhalts, die Zahl der erfassten Personendatensätze, der Zeitraum der erfassten Sachverhalte, die zusätzliche Heranziehung und Verknüpfung externer Daten bzw. Datensätze, die Einbeziehung der Daten dritter Personen, die Laufzeit des Forschungsvorhabens, die Art der Verarbeitung.

13. Bei der Güterabwägung ist auch von Bedeutung, wie viele Personen im Rahmen des Forschungsprojektes von den Daten Kenntnis erlangen (müssen) und welche **technisch-organisatorischen Maßnahmen** getroffen werden (§ 7). Die konkreten Datensicherungsmaßnahmen richten sich nach der Art der Daten und nach ihrer Verwendung; sie müssen sich auf die Gestaltung und den Ablauf des Projektes beziehen. Dies gilt für die Erhebungsphase (z. B. Hinweis auf Freiwilligkeit, Verhinderung des Einblicks Unbefugter), die Auswertungsphase (z. B. sichere Aufbewahrung der Daten, Festlegung der Zugriffsberechtigung) wie auch für den Abschluss des Projekts (z. B. Vernichtung des Rohmaterials, Datenlöschung).

14. Bei der Übermittlung von Sozialdaten für Forschungszwecke bedarf es der **Genehmigung** durch die oberste Bundes- oder Landesbehörde (§ 75 SGB X). In Niedersachsen ist dies zumeist das Niedersächsische Ministerium für Soziales, Frauen, Familie und Gesundheit. Einen entsprechenden Genehmigungsvorbehalt kennt das NDSG nicht. Stattdessen sieht das Gesetz zur Gewährleistung, dass die Abwägung den Intentionen des Gesetzes Rechnung trägt, eine spezielle Dokumenta-

tionspflicht und die **Unterrichtung der oder des behördlichen Datenschutzbeauftragten** vor. Die Unterrichtung hat in jedem Fall des § 25 Abs. 2 Nr. 3 (1. und 2. Alternative) zu erfolgen. Sie lässt die datenschutzrechtliche Verantwortung der forschenden Stelle unberührt.

Zu Abs. 3

15. Abs. 3 enthält die wichtige Klarstellung, dass die für ein Forschungsvorhaben genutzten Daten einer besonderen, **endgültigen Zweckbindung** unterliegen und daher nicht für andere als Zwecke der wissenschaftlichen Forschung weiterverarbeitet werden dürfen (Forschungsgeheimnis). Dies hat zur Folge, dass die Zweckbindungstatbestände des § 10 Abs. 2 Nr. 2 und Nr. 3 nicht zum Tragen kommen.

Zu Abs. 4

16. Es ist dafür Sorge zu tragen, dass die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, so früh wie möglich gesondert gespeichert bzw. gelöscht werden. Auswertungen dürfen nur aus den nicht personenbezogenen Datenbeständen erfolgen. Bedarf es in Einzelfällen der Reidentifizierung, so sollten die Identifikationskriterien abgetrennt und von einem Treuhänder oder einer/einem ausdrücklich hierzu ermächtigten Mitarbeiterin/Mitarbeiter verwaltet werden. Ein Treuhänder sollte von der forschenden Stelle unabhängig sein. Die Datei mit den Identifikationsmerkmalen muss spätestens gelöscht werden, wenn das Forschungsprojekt beendet ist.

Zu Abs. 5

17. Die **personenbezogene Veröffentlichung** der Forschungsergebnisse ist nur bei Einwilligung zulässig oder wenn dies für die Darstellung von Ereignissen der Zeitgeschichte unerlässlich ist. Eine Veröffentlichung ist eine Datenübermittlung an einen unbestimmten Empfängerkreis. Hinsichtlich der **Einwilligung** sind § 25 Abs. 6 und § 4 Abs. 2 und 3 anwendbar.

Zu Abs. 6

18. Die Erhebung wie auch jede weitere Verarbeitung hat vorrangig mit Einwilligung der Betroffenen zu erfolgen. Bei der **Einwilligung** sind Abs. 6 sowie § 4 Abs. 2 und 3 zu beachten. Eine wirksame Einwilligung liegt nur vor, wenn diese freiwillig erteilt worden ist. Voraussetzung jeder Einwilligung ist, dass die Betroffenen umfassend über das Forschungsprojekt (Zweck, Beteiligte, Form der Verarbeitung, Anonymisierung) unterrichtet werden. Die Betroffenen sind darüber zu unterrichten, dass die Teilnahme an der Befragung freiwillig ist, aus der Teilnahmeverweigerung keine Nachteile entstehen und die Einwilligung mit Wirkung für die Zukunft widerrufen werden kann. Es empfiehlt sich, anlässlich der Datenerhebung bei den Betroffenen ein Hinweisblatt mit den nötigen Angaben zu übergeben. Auch bei einem Vorhaben mit bei den Betroffenen erhobenen Daten müssen die sonstigen Datenschutzvorkehrungen für Forschungsprojekte beachtet werden. Verdeckte Datenerhebungen oder Täuschungen der Betroffenen über den Zweck der Erhebung sind unzulässig.

19. Die Vorschrift trägt dem Umstand Rechnung, dass in bestimmten Fällen das Verlangen einer schriftlichen **Einwilligung** der Betroffenen das Forschungsvorhaben erheblich beeinträchtigen kann. Insoweit verzichtet das Gesetz auf die geltenden Formvorschriften. Eine erhebliche Beeinträchtigung ist noch nicht gegeben, wenn nach Unterrichtung und Befragung der Betroffenen vereinzelt damit zu rechnen ist, dass einige zwar eine mündliche, nicht aber eine schriftliche Einwilligung erteilen würden. Beeinträchtigt wäre ein Vorhaben aber, wenn die Einholung der schriftlichen Einwilligung bei den Betroffenen zu einer Befangenheit führen würde, die sich auf deren korrekte Beantwortung der Fragen auswirken würde. Auf eine schriftliche Einwilligung muss u. U. auch verzichtet werden, wenn eine telefonische Befragung erfolgt. Die Vermeidung von Portokosten ist grundsätzlich kein Grund, der den Verzicht auf schriftliche Einwilligungen rechtfertigen könnte. Die Gründe der erheblichen Beeinträchtigung sollten schriftlich festgehalten werden. Die sonstigen Regelungen zur Einwilligung nach § 4 Abs. 2 und 3 sind zu beachten.

Zu Abs. 7

20. Abs. 7 regelt die **Übermittlung an private Stellen** zu Forschungszwecken sowie an öffentliche Stellen außerhalb des Geltungsbereichs des Gesetzes. Die §§ 11 und 13 bis 15 werden insoweit verdrängt. Voraussetzung ist in jedem Fall, dass es sich um ein konkretes wissenschaftliches Vorhaben handelt. Durch die Wendung "von ihnen zu bezeichnende" wird verdeutlicht, dass die Datenempfänger die Verpflichtung trifft, ihr Forschungsvorhaben konkret zu benennen, für das sie die Daten verarbeiten wollen. Da für diesen Kreis das NDSG nicht gilt, sind die Empfänger auf die Regelungen der Abs. 3 bis 5 zu verpflichten. Die Zweckbindung und weitere Verarbeitungsvorgaben müssen durch spezielle Absprachen gesichert werden. Diese Verpflichtung sollte in einem schriftlichen Vertrag erfolgen.

21. Die Anzeigepflicht gegenüber der oder dem Landesbeauftragten (Abs. 7 Satz 2) sorgt für Selbstkontrolle, Transparenz und ermöglicht gezielte Kontrollmaßnahmen oder weitere Interventionen, gegebenenfalls in Zusammenarbeit mit anderen Kontrollinstanzen, und zwar bevor die Verarbeitung erfolgt. Die Anzeige sollte so früh wie möglich, spätestens aber einen Monat vor Beginn der Verarbeitung erfolgen. Eine Pflicht der oder des Landesbeauftragten zur Reaktion auf die Unterrichtung besteht nicht.

§ 25 a
Beobachtung durch Bildübertragung

(1) Die Beobachtung öffentlich zugänglicher Räume durch Bildübertragung (Videoüberwachung) ist nur zulässig, soweit sie

1. zum Schutz von Personen, die der beobachtenden Stelle angehören oder diese aufsuchen, oder

2. zum Schutz von Sachen, die zu der beobachtenden Stelle oder zu den Personen nach Nummer 1 gehören,

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der von der Beobachtung betroffenen Personen überwiegen.

(2) [1]Die Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder die Betroffenen ausdrücklich eingewilligt haben.

(3) Die Möglichkeiten der Beobachtung und der Aufzeichnung sowie die verarbeitende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(4) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese über die jeweilige Verarbeitung zu unterrichten. [2]Von einer Unterrichtung kann abgesehen werden,

1. solange das öffentliche Interesse an einer Strafverfolgung das Unterrichtungsrecht der betroffenen Person erheblich überwiegt oder

2. wenn die Unterrichtung im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

(6) Dem Einsatz der Videoüberwachung muss stets eine Prüfung nach § 7 Abs. 3 vorausgehen.

Zu § 25 a

1. Die von vielen Behörden und anderen öffentlichen Stellen seit Jahren praktizierte, häufig auf das sogenannte Hausrecht gestützte Überwachung öffentlich zugänglicher Räume unter Einsatz von Videotechnik hat durch diese Regelung nunmehr eine ausdrückliche gesetzliche Grundlage erhalten (Gesetz zur Änderung des Niedersächsischen Verwaltungsverfahrensgesetzes und anderer Gesetze vom 16. Dezember 2004 – Nds. GVBl. S. 634).

Die Datenerhebung durch Videobeobachtung stellt aufgrund der hohen Informationsdichte einen besonders tiefen Eingriff in das Recht auf informationelle Selbstbestimmung der beobachteten Personen dar. Zwangsläufig werden Daten über viele unbeteiligte Personen sowie unabhängig vom Beobachtungszweck umfangreiche Zusatzinformationen aufgenommen (Kleidung, Gang, Gesichtsausdruck, Begleitpersonen usw.). Deshalb ist die Bestimmung zu begrüßen, da sie einen angemessenen Ausgleich zwischen dem Interesse der beobachtenden Stelle und den beobachteten Personen schafft.

Die Bestimmung erlaubt nur Bildaufnahmen. Tonaufnahmen sind nicht zulässig und können im Einzelfall zu einer strafrechtlichen Verfolgung gemäß § 201 Strafgesetzbuch (StGB) führen.

Der Hauptanwendungsfall der Regelung ist die Videoüberwachung der öffentlichen Gebäude des Landes, der Kommunen sowie der anderen gemäß § 2 NDSG dem Anwendungsbereich dieses Gesetzes unterliegenden Stellen.

2. Bereichsspezifische Regelungen zum Einsatz der Videotechnik, wie z. B. nach § 32 Abs. 3 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) oder dem Gesetz über den Verfassungsschutz im Lande Niedersachsen (NVerfSchG), bleiben ebenso unberührt wie die Vorschriften des § 6 b BDSG zur Videoüberwachung für den gewerblichen und privaten Bereich.

Nur Abfallbehörden als zuständige Behörden gemäß § 41 i. V. m. § 45 Abs. 2 des Niedersächsischen Abfallgesetzes (NAbfG) nicht jedoch öffentlich-rechtliche Versorgungsträger gemäß § 6 i. V. m. § 45 Abs. 1 NAbfG dürfen u. a. Wertstoffhöfe per Video überwachen (simultan beobachten), sofern dies zur Gefahrenabwehr (illegale Müllentsorgung) erforderlich ist. Eine Aufzeichnung der übertragenen Bilder ist allerdings nicht zulässig (vgl. § 45 Abs. 2 NAbfG i. V. m. den §§ 1 Abs. 1 und § 32 Abs. 3 des Nds. SOG).

3. Bei dem Einsatz von dauerhaft defekten Kameras und Attrappen, so genannter „Dummies“, findet keine Bildübertragung statt. Somit werden keine Daten verarbeitet und das NDSG ist daher nicht einschlägig.

Diese Kameravarianten greifen zwar nicht in das Recht auf informationelle Selbstbestimmung, wohl aber in das Recht auf freie Entfaltung der Persönlichkeit der Betroffenen ein (Art. 2 Abs. 1 GG), da sie zu einer Verhaltensbeeinflussung führen. Eine Rechtsgrundlage für diesen Eingriff ist nicht ersichtlich.

Problematisch wird es für die verantwortliche Stelle spätestens, wenn sich Betroffene an die vermeintlich videoüberwachende Stelle wenden, um z. B. auf das Fehlen

"geeigneter Maßnahmen" gemäß § 25 a Abs. 3 NDSG hinzuweisen und/oder um Auskunft nach § 16 NDSG und Einsicht in die Verfahrensbeschreibung nach § 8 a Abs. 3 Satz 1 NDSG zu verlangen. Die Behörde müsste zugeben, rechtswidrig gehandelt zu haben, indem sie etwas behauptet hat („Hier wird videoüberwacht“), von dem sie weiß, dass es nicht zutrifft.

4. Die Beobachtung nicht öffentlich zugänglicher Räume in öffentlichen Gebäuden wird nicht von dieser Norm erfasst. Öffentlich nicht zugänglich sind Räume, wenn nur ein zuvor definierter enger Personenkreis (z. B. Mitarbeiterinnen und Mitarbeiter, Schülerinnen und Schüler, usw.) Zugang zu diesem Raum haben, vgl. folgende Beispiele:

- Büros von Beschäftigten;
- Ausstellungsräume von Museen nach der abendlichen Schließung;
- Die Aula einer Schule bei schulinternen Veranstaltungen (bei einem Schulkonzert, dessen Besuch auch nicht der Schule angehörenden Personen offen steht, ist die Aula dagegen öffentlich zugänglicher Raum).

Dieser eingegrenzte Personenkreis befindet sich, anders als in der „allgemeinen Öffentlichkeit“, in diesen Räumen generell in einer bestimmten „Rolle“. Die Gefahr, durch diese Art der Videoüberwachung in den allgemeinen Lebensäußerungen und Verhaltensweisen beeinflusst zu werden, ist also vergleichsweise geringer als bei der Videoüberwachung in öffentlich zugänglichen Räumen.

Dennoch müssen auch hier bestimmte Voraussetzungen erfüllt sein:

a) Der Zweck der Videoüberwachung ist genau zu definieren;
b) Die Erforderlichkeit des Videoeinsatzes muss festgestellt werden, d. h., es dürfen keine anderen zumutbaren Möglichkeiten bestehen, den beabsichtigten Zweck der Videoüberwachung zu erreichen;
c) Es ist eine Vorabkontrolle durchzuführen. § 7 Abs. 3 NDSG bestimmt, dass ein automatisiertes Verfahren nur eingesetzt oder wesentlich verändert werden darf, soweit Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien entstehen können, durch Maßnahmen nach Abs. 1 wirksam beherrscht werden können;
d) Die zu treffenden Feststellungen sind schriftlich festzuhalten;
e) Durch technisch-organisatorische Maßnahmen ist sicherzustellen, dass die erhobenen Daten nur zu dem definierten Zweck ausgewertet oder sonst verarbeitet werden. Insbesondere ist sicherzustellen, dass die Daten nicht für eine Leistungs- und/oder Verhaltenskontrolle der Betroffenen genutzt werden;
f) Der Personenkreis, der Zugang zu den Daten hat, ist abschließend zu definieren;
g) Es ist sicherzustellen, dass die gespeicherten Daten jeweils am auf die Aufzeichnung folgenden Arbeitstag gelöscht werden, es sei denn, eine weitere

Speicherung ist im Einzelfall erforderlich, weil Beschädigungen, Diebstahl o. ä. (Zweck der Videoüberwachung) festgestellt wurden;

h) Auf die Videoüberwachung ist in der Nähe des Raumes deutlich hinzuweisen. Die Nutzer müssen in der Lage sein, den Hinweis erkennen zu können, bevor sie den überwachten Raum betreten;

i) Beteiligungsrechte (z. B. Personalvertretung, Schulkonferenz) sind zu beachten.

Zu Absatz 1

5. Die Regelung nennt die Zulässigkeitsvoraussetzungen, die kumulativ vorliegen müssen.

Eine Legaldefinition für den Begriff öffentlich zugänglicher Räume gibt es nicht. Als öffentlich zugängliche Räume im Sinne dieser Vorschrift sind nicht nur umbaute, sondern auch unter freiem Himmel befindliche Flächen anzusehen, die nach ihrem Zweck bestimmt bzw. ausdrücklich dafür gewidmet sind, von einer unbestimmten Zahl von Personen oder einem nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten oder genutzt zu werden. Dabei ist es unerheblich, ob ein Eintrittsgeld für das Betreten der Räume zu zahlen oder ein kostenloser Zutritt möglich ist. Auch etwaige Altersbegrenzungen oder sonstige Bedingungen („Zutritt nur in Begleitung Erwachsener“) sind in diesem Zusammenhang unerheblich. Beispiele öffentlich zugänglicher Räume sind öffentliche Badeanstalten, Kinderspielplätze oder öffentliche Sportplätze, aber auch Eingangs- und Publikumsbereiche in Rathäusern und sonstigen öffentlichen Gebäuden sowie Ausstellungsräume in Museen.

Öffentlicher Verkehrsraum darf in die Überwachung nur einbezogen werden, wenn es sich um unmittelbar angrenzende Verkehrsflächen handelt (z. B. Fußweg vor der Fassade eines öffentlichen Gebäudes).

6. Die Beobachtung ist nur zur Verfolgung eines oder der beiden unter Nummern 1 und 2 genannten Zwecke (Schutz von Personen oder Sachen, die in einer Verbindung zu der beobachtenden Stelle stehen), die u. a. in der Verfahrensbeschreibung festgelegt werden müssen, zulässig; die Beobachtung muss zudem zur Zweckerreichung geeignet, erforderlich und angemessen sein und somit dem allgemeinen Verhältnismäßigkeitsgrundsatz entsprechen. Wegen des erheblichen Eingriffs in die Privatsphäre der betroffenen Personen ist eine Beobachtung nur verhältnismäßig, wenn der beabsichtigte Zweck mit zumutbaren anderen Mitteln wie z. B. verstärkten Kontrollen durch Personal, bauliche Umgestaltungen o. ä. nicht ebenfalls erreicht werden kann.

7. Sofern die Zulässigkeitsvoraussetzungen der Videoüberwachung im Einzelfall als gegeben festgestellt worden sind, hat die Daten verarbeitende (beobachtende) Stelle vor Beginn der Überwachung in einem weiteren Schritt zu prüfen, ob nicht überwiegende schutzwürdige Interessen der von der Beobachtung betroffenen Personen einer Videobeobachtung entgegenstehen. Da bereits mit der bloßen Beobachtung, also auch ohne Aufzeichnung, Verhaltensweisen der beobachteten Personen zur Kenntnis genommen werden können (Datenerhebung) und sich die beobachteten

Personen dadurch hinsichtlich ihres Verhaltens u. a. einem „latenten Anpassungsdruck“ ausgesetzt sehen, ist eine Abwägung zwischen den Interessen der beobachtenden Stelle an der Durchführung der Videobeobachtung und den Interessen der betroffenen Personen an der Nichtbeobachtung vorzunehmen. Überwiegen bei dieser Abwägung die Interessen der betroffenen Personen, ist die Videobeobachtung unzulässig. Dies ist in aller Regel anzunehmen, wenn die Videoüberwachung Bereiche erfasst, die dem höchstpersönlichen oder Intimbereich der beobachteten Personen zuzuordnen sind; daher ist etwa die Videoüberwachung von Toiletten, Duschen oder Umkleideräumen unzulässig.

Zu Absatz 2

8. Inhalt dieser Regelung ist die weitere Verarbeitung der nach Absatz 1 erhobenen Daten, die vor allem in der Speicherung des Bildmaterials durch die Daten verarbeitende Stelle besteht. Für die Zulässigkeit der weiteren Verarbeitung sind erneut die gleichen rechtlichen Voraussetzungen zu prüfen wie bei der reinen Beobachtung nach Absatz 1. Dabei muss das Erreichen des verfolgten Zweckes auch gerade die Speicherung der Bilddaten erfordern und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen an der Nichtspeicherung überwiegen.

9. Nach Satz 2 darf das gespeicherte Bildmaterial für einen anderen Zweck – abweichend vom Zweck der Beobachtung und der Speicherung gemäß Abs. 1 und Abs. 2 Satz 1 – nur dann verarbeitet werden, soweit dies zur Abwehr von (anderen) Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder die Betroffenen ausdrücklich eingewilligt haben.

10. Der Daten verarbeitenden Stelle obliegt die fortwährende Verpflichtung zur Prüfung, ob die Voraussetzungen für die Videoüberwachung und die weitere Verarbeitung der Bilddaten noch gegeben sind. Ist dies nicht mehr der Fall, ist die Überwachung einzustellen und die Videoanlage abzubauen, gespeicherte Bilddaten sind zu löschen.

Zu Absatz 3

11. Das Transparenzgebot verpflichtet die für die Videoüberwachung verantwortliche Stelle, die von der Beobachtung betroffenen Person auf die Möglichkeit bzw. den Umstand der Beobachtung und ggf. Aufzeichnung durch geeignete Maßnahmen, also z. B. durch deutlich sichtbare Piktogramme oder Texttafeln, hinzuweisen. Da die betroffene Person die Möglichkeit haben muss, dem beobachteten Raum ausweichen zu können, ist das Piktogramm bzw. die Hinweistafel so anzubringen, dass die betroffene Person vor dem Betreten des beobachteten Raumes davon eindeutig Kenntnis nehmen können. Von besonderen Hinweisen kann abgesehen werden, wenn der Umstand der Beobachtung und ggf. der Aufzeichnung auch so eindeutig und frühzeitig erkannt werden kann; da die Kameras immer kleiner und leistungsfähiger werden und auch durch veränderte Bauformen häufig kaum noch als solche erkannt werden können, dürfte dies nur ausnahmsweise gegeben sein.

In allen Fällen muss ein Hinweis auf die für die Beobachtung verantwortliche Stelle (Name der Behörde, Erreichbarkeit, ggf. Ansprechpartner) vorhanden sein.

Zu Absatz 4

12. Die Regelung des Satzes 1 stellt sicher, dass die Person, deren Recht auf informationelle Selbstbestimmung durch die Zuordnung und Verarbeitung von durch Videobeobachtung erhobenen Daten in besonderer Weise beeinträchtigt wird, hierüber individuell zu unterrichten ist, damit sie ggf. ihre datenschutzrechtlichen Rechte wahrnehmen kann. Sofern die Daten auch an Dritte übermittelt werden, umfasst die Unterrichtung der Betroffenen auch den Namen der Datenempfänger.

Satz 2 benennt die Fälle, in denen ausnahmsweise eine Benachrichtigung der Betroffenen unterbleiben kann.

Zu Absatz 5

13. Aus dem Löschungsgebot ergibt sich für die verantwortliche Stelle die Verpflichtung, unverzüglich zu prüfen, ob das angefallene Videomaterial zur Zweckerreichung weiterhin erforderlich ist. Anderenfalls ist es zu löschen.

Die Prüfung kann z. B. bei einer Überwachung der Außenwand eines Gebäudes dadurch erfolgen, dass vor Ort überprüft wird, ob es Beschädigungen gegeben hat. In anderen Fällen kann eine Sichtung des aufgezeichneten Videomaterials angezeigt sein. Generell wird unter dem Aspekt der Zweckerreichung eine Überprüfung schon nach kurzen Zeitabständen von wenigen Stunden erforderlich sein, z. B. um mögliche Täter möglichst umgehend zu erkennen und geeignete Maßnahmen zu ihrer Identifikation bzw. Ergreifung einleiten zu können. In anderen Fällen wird eine Speicherung bis zum Ablauf des folgenden Arbeitstages zulässig sein, um so beispielsweise eine Überprüfung der Ereignisse des vergangenen Wochenendes zu ermöglichen, wenn hierfür entsprechend dem definierten Zweck Anlass besteht.

Nach der Überprüfung darf nach Absatz 2 gewonnenes Videomaterial nur noch insoweit gespeichert bleiben, als es sich um relevante Aufnahmen handelt, die für den Beobachtungszweck (z. B. zur Strafverfolgung) weiterhin benötigt werden und deren weitere Speicherung schutzwürdigen Interessen der Betroffenen nicht entgegenstehen.

Zu Absatz 6

14. Durch diese Regelung wird gewährleistet, dass bei jedem Einsatz von Videoüberwachungsanlagen sowohl nach dem NDSG als auch nach spezialgesetzlichen Regelungen eine Vorabkontrolle nach § 7 Absatz 3 durch die behördliche Beauftragte oder den behördlichen Beauftragten für den Datenschutz erfolgt. Dabei spielt es keine Rolle, ob eine analoge oder digitale Technik zur Beobachtung oder zur Beobachtung mit Aufzeichnung eingesetzt wird. Insbesondere ist zu prüfen und zu dokumentieren, welche Gesichtspunkte mit welchem Ergebnis in die nach Abs. 1 und 2 vorzunehmende Interessenabwägung einzubeziehen sind, durch welche Maßnahmen und Vorkehrungen sichergestellt werden kann, dass nur berechtigte Personen zu den festgelegten Zwecken in die Videoüberwachung eingebunden werden und Zugang zu

den Bilddaten erhalten, und wie die gesetzlichen Vorgaben zur Erkennbarmachung nach Abs. 3 sowie zur Löschung nach Abs. 5 im konkreten Fall sachgerecht umgesetzt werden können.

§ 26
Fernmessen und Fernwirken

(1) [1]Ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) dürfen in Wohnungen oder Geschäftsräumen nur vorgenommen werden, wenn die Betroffenen zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden sind und nach der Unterrichtung schriftlich eingewilligt haben. [2]Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen Wirkungen auszulösen (Fernwirkdienste). [3]Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn die Betroffenen erkennen können, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist. [4]Die Betroffenen können ihre Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. [5]Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) [1]Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht von der Einwilligung nach Absatz 1 abhängig gemacht werden. [2]Betroffenen dürfen keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen, wenn sie ihre Einwilligung verweigern oder widerrufen.

(3) [1]Die im Rahmen von Fernmess- oder Fernwirkdiensten erhobenen Daten dürfen nur zu den vereinbarten Zwecken verarbeitet werden. [2]Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

Zu Abs. 1

1. Das Fernmessen in der Sphäre der Betroffenen stellt eine Datenerhebung, das Fernwirken eine Datenübermittlung und Datenspeicherung dar.

Fernmessen und Fernwirken sind **nur mit Einwilligung** der Betroffenen zulässig. Das technische Verfahren ist dabei so zu gestalten, dass die Betroffenen erkennen können, wann ein Dienst in Anspruch genommen wird. Dadurch erhalten sie die Möglichkeit, durch Abschalten des Dienstes bei Verdacht des Missbrauchs ihr jederzeitiges Widerrufsrecht unmittelbar wahrnehmen zu können.

Zu Abs. 2 und 3

2. Es ist nicht erlaubt, eine Leistung oder den Abschluss eines Vertrages davon abhängig zu machen, dass die Betroffenen ihre Einwilligung erteilen.

Das folgende Beispiel verdeutlicht die Intention der Regelung, jedoch ist zu beachten, dass für Stromlieferanten heutzutage in der Regel das BDSG Anwendung finden wird:

Nicht zulässig wäre es, den Abschluss eines Stromlieferungsvertrages von der Einwilligung in die Nutzung der Leitungen zu Mess- oder Abrechnungszwecken abhängig zu machen. Sollten derartige Verfahren eingeführt werden, so wäre immer

auch eine andere Möglichkeit der Verbrauchsmessung vorzusehen. Den Betroffenen dürfen keine über die unmittelbar entstehenden Folgekosten hinausgehenden Nachteile aus einer nicht erteilten Einwilligung entstehen, damit sie nicht in ihrer freien Willensentscheidung beeinträchtigt sind.

Absatz 3 betont nochmals ausdrücklich das allgemein gültige Gebot der Zweckbindung und der frühestmöglichen Löschung.

§ 27
Öffentliche Auszeichnungen

(1) [1]Zur Vorbereitung öffentlicher Auszeichnungen dürfen die dazu erforderlichen personenbezogenen Daten auch ohne Kenntnis der Betroffenen bei anderen Personen oder Stellen erhoben werden. [2]Auf Anforderung dürfen öffentliche Stellen die erforderlichen Daten übermitteln.

(2) § 16 findet keine Anwendung.

Zu § 27

Zur Vorbereitung der Verleihung öffentlicher Auszeichnungen ist es zulässig, personenbezogene Daten auch ohne Kenntnis der Betroffenen zu erheben und zu verarbeiten. Um das Verfahren nicht zu gefährden, sind Ausnahmen von den allgemeinen Datenschutzgrundsätzen der Erhebung beim Betroffenen und dem Auskunftsrecht geschaffen worden.

Sechster Abschnitt

Übergangs- und Schlussvorschriften

§ 28
Straftaten

(1) [1]Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten, die nicht allgemein zugänglich sind,

1. **unbefugt erhebt, speichert, verändert, löscht, übermittelt oder nutzt oder**
2. **durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,**

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Der Versuch ist strafbar.

Zu § 28

1. Die Vorschrift dient dem Schutz der Betroffenen gegen bestimmte Formen des unbefugten Umgangs mit ihren personenbezogenen Daten. Geschützes Rechtsgut ist nicht das einzelne Datum, sondern die Privatsphäre. Diese Regelung soll eine ergänzende Ahndungsmöglichkeit für Verhaltensweisen bieten, bei denen eine Sanktion angezeigt erscheint und die durch andere Strafvorschriften nicht erfasst werden (z. B. §§ 202a, 203, 269, 270, 303 a, 303 b, 353 b StGB, § 17 UWG).

Zu Abs. 1

2. Als Täter kommt nur eine Person in Betracht, die personenbezogene Daten der öffentlichen Stelle (Normadressat des NDSG) verarbeitet oder nutzt.

Da § 28 – anders als die Regelung des § 29 – keinen Bezug auf § 5 nimmt, ist nicht erforderlich, dass der Täter dem Datengeheimnis unterliegt. An dessen Verletzung ist keine eigenständige strafrechtliche Sanktion geknüpft. Sie kann allenfalls als Ordnungswidrigkeit geahndet werden (s. § 29 Abs. 1 Nr. 1).

3. Die unbefugte Verarbeitung oder Nutzung von Daten ist nur strafbar, wenn der Täter **gegen Entgelt** bzw. in **Bereicherungs- oder Schädigungsabsicht** handelt. Auf diese Weise sollen nur qualifizierte Verstöße als strafbares Unrecht gewertet werden. Entgelt ist nach § 11 Abs. 1 Nr. 9 StGB, Art. 1 Abs. 2 EGStGB jede in einem Vermögensvorteil bestehende Gegenleistung; auf eine Bereicherung kommt es nicht an. Für die Bereicherungs- oder Schädigungsabsicht genügt, dass es dem Täter auf die Bereicherung oder Schädigung ankommt, wobei sie nicht das maßgebliche Ziel

oder der letzte Zweck zu sein braucht. Die angestrebte Bereicherung muss rechtswidrig sein, d. h. es darf kein Anspruch auf sie bestehen. Der Täter muss die Rechtswidrigkeit kennen. Absicht ist insoweit nicht erforderlich.

4. Tatobjekt sind personenbezogene Daten, die dem Anwendungsbereich des NDSG unterfallen (§ 2) und „nicht allgemein zugänglich sind“. Dabei ist gleichgültig, ob es sich um automatisiert oder manuell verarbeitete personenbezogene Daten handelt.

Für Daten, die von Beschäftigten der in § 2 Abs. 2 und 4 genannten juristischen Personen des öffentlichen Rechts, deren Einrichtungen, Eigenbetrieben sowie öffentlich-rechtlichen Kreditinstituten und Versicherungsanstalten verarbeitet werden, gelten die Straf- und Bußgeldvorschriften der §§ 43, 44 BDSG. Das gilt auch, soweit es sich um personenbezogene Daten handelt, die nicht in den Anwendungsbereich des NDSG fallen. Schließlich verdrängen spezielle Strafvorschriften gemäß § 2 Abs. 6 die Regelung des § 28. Zu nennen sind z. B. die Vorschriften der § 22 BStatG, § 85 a SGB X oder § 12 NStatG.

5. Voraussetzung für die Verwirklichung des Tatbestandes war bisher, dass die personenbezogenen Daten, die unbefugt verarbeitet wurden, „nicht offenkundig“ waren. **Offenkundigkeit** ist nach der Rechtsprechung allerdings bereits dann gegeben, wenn personenbezogene Daten bei Vorliegen bestimmter im Einzelnen geregelter Voraussetzungen an jedermann übermittelt werden können. Auf der Grundlage dieser Rechtsauffassung konnten z. B. unbefugte Abrufe aus dem zentralen Informationssystem des Kraftfahrtbundesamtes durch einzelne öffentliche Bedienstete und die Weitergabe dieser Daten an private Stellen strafrechtlich nicht geahndet werden. Durch die Änderung des Gesetzes soll sichergestellt werden, dass bei Vorliegen der sonstigen Voraussetzungen des § 28 eine strafrechtliche Ahndung nur in denjenigen Fällen ausgeschlossen ist, in denen es sich um Daten handelt, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang aus Gründen des Persönlichkeitsschutzes rechtlich beschränkt ist.

6. Die Tathandlungen des Satz 1 Nr. 1 sind im Sinne der Legaldefinitionen des § 3 Abs. 2 Satz 2 Nr. 1 bis Nr. 4, Nr. 6 und Nr. 7 zu verstehen. Nicht erfasst wird das unbefugte Sperren von Daten, da insoweit keine schutzwürdigen Belange beeinträchtigt werden. Zwar liegt ein Verändern vor, wenn allgemein zugängliche Daten (z. B. aus Telefonbüchern) in der Weise kombiniert werden, dass ein neuer Informationsgehalt entsteht (z. B. die Speicherung von Daten aus Telefonbüchern auf CD-Rom mit Such- und Selektionsmöglichkeiten). Dieses Verändern ist jedoch straflos, da es sich um Daten handelt, die zum Zeitpunkt der Tat allgemein zugänglich waren. Die spätere Einstufung der veränderten Daten als nicht allgemein zugänglich ist insoweit ohne Belang. Eine unbefugte Datenübermittlung kann auch dann vorliegen, wenn gebotene Schutzvorkehrungen unter Verletzung einer Garantenpflicht (§ 13 StGB, Art. 1 Abs. 2 EGStGB) unterlassen werden.

7. Satz 1 Nr. 2 erfasst das „Erschleichen“ personenbezogener Daten. Es handelt sich um die unbefugte Übermittlung von Daten in mittelbarer Täterschaft, wobei der Täter die Person, die für die verantwortliche Stelle (§ 3 Abs. 3) tätig wird, als „Werkzeug“ einsetzt. Dabei spiegelt er falsche Tatsachen vor, d. h. solche, die in Wirklichkeit nicht

gegeben sind, um den Tatmittler auf diese Weise zur Weitergabe der Daten an sich oder andere Personen zu veranlassen. Als Beispiele sind die Verwendung falscher Namens- oder Identitätsmerkmale, die Vorgabe einer Behördenzugehörigkeit, die Angabe eines unrichtigen Passwortes oder das Vortäuschen eines berechtigten bzw. rechtlichen Interesses zu nennen. Die Tathandlung knüpft lediglich an die erste Alternative des § 3 Abs. 2 Satz 2 in Nr. 4 a) an. Veranlasst der Täter, dass das „Werkzeug“ infolge der Täuschung ihm oder einem Dritten die Einsicht in oder den Abruf von Daten ermöglicht (§ 3 Abs. 2 Satz 2 Nr. 4 b), scheidet eine Strafbarkeit aus. Auf Grund des Wortlauts gilt dies auch, soweit der Täter lediglich wahre Tatsachen entstellt oder unterdrückt (vgl. § 263 Abs. 1 StGB). Insoweit besteht eine Strafbarkeitslücke.

8. Satz 2 regelt das sog. **Deanonymisieren** von Daten. Tatobjekt sind hier nicht personenbezogene Daten (§ 3 Abs. 1), sondern „Einzelangaben über persönliche und sachliche Verhältnisse einer nicht mehr bestimmbaren Person“. Ist die Bestimmbarkeit der Person infolge der Anonymisierung lediglich erschwert (vgl. § 3 Abs. 6 BDSG), liegen weiterhin personenbezogene Daten vor

9. Strafbar ist nur die vorsätzliche Begehung (§ 15 StGB, Art. 1 Abs. 2 EGStGB), die zudem unbefugt erfolgt sein muss. Die Befugnis, die sich gemäß § 4 aus den §§ 9 ff. oder anderen Rechtsvorschriften sowie aus der Einwilligung des Betroffenen ergeben kann, ist als Rechtfertigungsgrund anzusehen. Der Täter muss schließlich schuldhaft handeln.

10. Zuständige Verfolgungsbehörde ist die Staatsanwaltschaft (§ 152 Abs. 1 StPO). In der Praxis wird grundsätzlich zunächst die Polizei tätig, die zunächst die Straftat aufzuklären versucht (§ 163 Abs. 1 StPO) und dann das Ergebnis ihrer Nachforschungen der Staatsanwaltschaft vorlegt (§ 163 Abs. 2 Satz 1 StPO).

Zu Abs. 2

11. Strafbar ist nicht lediglich die vollendete Tat, sondern bereits das unmittelbare Ansetzen zur Verwirklichung des Tatbestandes im Sinne von Absatz 1 (vgl. § 23 Abs. 1 StGB, Art. 1 Abs. 2 EGStGB).

§ 29
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. **entgegen § 5 zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeitet oder offenbart oder**
2. **sich durch Vortäuschung falscher Tatsachen verschafft oder an sich oder andere übermitteln lässt.**

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden.

Zu § 29

1. Die Vorschrift soll bestimmte Verhaltensweisen bei der Verarbeitung von personenbezogenen Daten, die nicht als verwerfliches und damit strafwürdiges Unrecht angesehen werden, als **Ordnungswidrigkeit** (§ 1 Abs. 1, § 2 OWiG) sanktionieren. Das beruht auf der Überlegung, das Strafrecht nur dort einzusetzen, wo es unabdingbar erscheint (ultima ratio).

Zu Abs. 1

2. Täter kann grundsätzlich jedermann sein („wer“). Das gilt nicht für Tathandlungen nach Nr. 1. Diese können nur von Personen begangen werden, „die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben“ (§ 5 Satz 1). Erfasst werden Beschäftigte von Behörden und sonstigen öffentlichen Stellen sowie sog. beliehene Unternehmer (§ 2 Abs. 1), aber auch Mitarbeiter von privaten Unternehmen und Betrieben, die „im Auftrag öffentlicher Stellen“ personenbezogene Daten verarbeiten (§ 6). Sie haben dienstlichen Zugang zu personenbezogenen Daten, wenn sie sich im Rahmen ihrer Beschäftigung bei der öffentlichen Stelle bzw. dem Auftragnehmer (§ 3 Abs. 4) Kenntnis von den Daten verschaffen können. Dem „Datengeheimnis“ unterliegen auch Personen, die ihre Tätigkeit bei der öffentlichen Stelle bzw. dem Auftragnehmer beendet haben (§ 5 Satz 2). Auch diese können Täter einer Ordnungswidrigkeit gemäß § 29 Abs. 1 Nr. 1 sein.

3. Tatobjekt sind personenbezogene Daten (§ 3 Abs. 1), die in den Anwendungsbereich des NDSG (§ 2) fallen und „nicht allgemein zugänglich sind“. Dabei spielt es keine Rolle, ob es sich um automatisiert oder manuell verarbeitete Daten handelt. Insoweit kann auf die Anmerkungen zu § 28 verwiesen werden. Spezielle Vorschriften über Ordnungswidrigkeiten gehen auch hier der allgemeinen Regelung vor (§ 2 Abs. 6).

4. Die Tathandlung der Nr. 1 besteht im Verarbeiten oder Offenbaren von personenbezogenen Daten „zu einem anderen als dem zur (...) Aufgabenerfüllung notwendi-

gen Zweck“ (vgl. § 5 Satz 1). Während sich der Begriff der Verarbeitung an § 3 Abs. 2 anlehnt, kommt dem Wort „Offenbaren“ kein eigenständiger Bedeutungsgehalt zu, da es sich insoweit um die veraltete Beschreibung des Übermittelns von Daten im Sinne von § 3 Abs. 2 Satz 2 Nr. 4 handelt. Der Täter muss personenbezogene Daten zweckwidrig, d. h. für andere als zur befugten Aufgabenerfüllung gehörende Zwecke verarbeiten, so z. B. wenn ein Mitarbeiter der Meldebehörde Daten aus dem Melderegister kopiert, um sie für eine private Versicherungstätigkeit zu verwenden. Für diese Zweckdurchbrechung gibt es weder eine Fiktion der Zweckwahrung (vgl. § 10 Abs. 3) noch eine gesetzliche Befugnis zur Zweckdurchbrechung oder eine Einwilligung der Betroffenen (vgl. § 10 Abs. 2).

5. Die Tathandlung der Nr. 2 ist zunächst das **Verschaffen von Daten** durch Vorspiegeln falscher, d. h. unrichtiger Tatsachen. Verschaffen erfasst jede Art des Zugriffs auf personenbezogene Daten (Alt. 1). Nicht notwendig ist, dass der Täter den Datenträger (Diskette oder Akte) entwendet. Es genügt bereits das Abschreiben, Ablichten oder Kopieren der Daten, also jede Kenntnisnahme von den Informationen durch ein Handeln des Täters. Als Beispiel ist der Fall zu nennen, dass sich der Täter als Mitarbeiter einer Aufsichtsbehörde ausgibt, um bestimmte Akten einsehen und abschreiben zu können. Die Nr. 2 sanktioniert aber auch die Übermittlung von Daten in mittelbarer Täterschaft (Alt. 2), indem der Täter einen anderen z. B. über seine Identität täuscht und auf diese Weise erreicht, dass ihm das „Werkzeug“ personenbezogene Daten per E-Mail übersendet. Die Tathandlung knüpft an die Bekanntgabe von Daten im Sinne von § 3 Abs. 2 Satz 2 Nr. 4 a) und b) an. Bei dieser Alternative übermittelt das „Werkzeug“ selbst die Daten an den Täter, es „gibt“ die Daten heraus, während der Täter bei der ersten Alternative sich die Daten selbst „nimmt“, indem er sie fotokopiert oder abschreibt. Nicht erfasst wird wiederum das Entstellen oder Unterdrücken wahrer Tatsachen (vgl. § 263 Abs. 1 StGB).

6. Verfolgbar ist grundsätzlich nur das **vorsätzliche Handeln oder Unterlassen**, außer wenn das Gesetz fahrlässiges Handeln ausdrücklich mit Geldbuße bedroht (§ 10 i. V. m. § 2 OWiG). Auch der Versuch kann nur geahndet werden, wenn das Gesetz es ausdrücklich zulässt (§ 13 Abs. 2 OWiG).

7. Sachlich zuständig für die Verfolgung und Ahndung einer Ordnungswidrigkeit nach § 29 des NDSG ist die jeweilige Aufsichtsbehörde bei Zuwiderhandlungen durch Beschäftigte der Daten verarbeitenden Stelle, jedoch die Daten verarbeitende Stelle selbst, wenn sie als oberste Landesbehörde keiner behördlichen Aufsicht untersteht oder wenn ihre unmittelbare Aufsichtsbehörde eine oberste Landesbehörde ist (§ 7 Nr. 11 ZustVO-OWi). Der oder dem Landesbeauftragten für den Datenschutz kommt insoweit keine Zuständigkeit zu (vgl. §§ 22, 23).

Zu Abs. 2

8. Das Höchstmaß der angedrohten **Geldbuße** beträgt bis zu 50 000 Euro (§ 17 Abs. 1, § 2 OWiG, § 29 Abs. 2 NDSG). Ob ein Verstoß gegen § 29 Abs. 1 NDSG mit einer Geldbuße geahndet wird, steht im Ermessen der zuständigen Behörde („kann“). Grundlage der Zumessung der Geldbuße sind die Bedeutung der Ordnungswidrigkeit und der Vorwurf, der den Täter trifft. Auch die wirtschaftlichen Verhältnisse des Täters

kommen in Betracht; bei geringfügigen Ordnungswidrigkeiten bleiben sie jedoch in der Regel unberücksichtigt (§ 17 Abs. 3, § 2 OWiG).

Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten

Vom 10. Juli 2002 (Nds. GVBl. S. 349)

Aufgrund des § 8 a Abs. 5 des Niedersächsischen Datenschutzgesetzes (NDSG) in der Fassung vom 29. Januar 2002 (Nds. GVBl. S. 22), wird verordnet:

§ 1

Für automatisierte Verarbeitungen, von denen nach § 2 eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Betroffenen nicht zu erwarten ist, bedarf es abweichend von § 8 a Abs. 1 NDSG nicht der Bestellung einer oder eines Beauftragten für den Datenschutz.

§ 2

(1)[1]Verarbeitungen, von denen eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Betroffenen nicht zu erwarten ist, sind die ausschließlich zweckgebundenen automatisierten Verarbeitungen personenbezogener Daten

1. zur Abwicklung der Amtstätigkeit und der Dienstgeschäfte der Notarinnen und Notare sowie der Beschäftigungsverhältnisse der bei ihnen beschäftigten Personen,
2. für Zwecke der Textverarbeitung einschließlich der Übermittlung dieser Dokumente in automatisierter Form, soweit die personenbezogenen Daten von der Daten verarbeitenden Stelle nur für Zwecke der Dokumentation des Schriftwechsels und der Übermittlung automatisiert gespeichert werden.

[2]Satz 1 Nr. 2 gilt nicht, soweit Daten im Sinne des § 4 Abs. 2 Satz 2 NDSG verarbeitet werden.

(2) [1]In den Fällen des Absatzes 1 Satz 1 Nr. 2 dürfen die personenbezogenen Daten nur so lange aufbewahrt werden, wie ihre Kenntnis für die Daten verarbeitende Stelle erforderlich ist. [2]§ 17 Abs. 2 Satz 3 NDSG gilt entsprechend.

§ 3

Diese Verordnung tritt am Tage nach ihrer Verkündung in Kraft.

Hannover, den 10. Juli 2002

Die Niedersächsische Landesregierung

Verwaltungsvorschriften zum Niedersächsischen Datenschutzgesetz (VV NDSG)

Gem. RdErl. des MI, der StK u. d. übr. Min. vom 26.06.2002 (Nds. MBl. S. 640)

-VORIS 20600 02 00 00 001-

Bezug: Gem. RdErl. v. 23.06.1994 (Nds. MBl. S. 1147), geändert durch
Gem. RdErl. v. 11.05.1998 (Nds. MBl. S. 920)
- Voris 20600 02 00 00 001 -

Zu § 2 (Anwendungsbereich)

1.1

Neben den öffentlichen Stellen im engeren Sinne findet das NDSG auch Anwendung auf Vereinigungen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, die privatrechtlich (z. B. als eingetragener Verein oder GmbH) organisiert sind (vgl. § 2 Abs. 2 BDSG). Um eine Vereinigung in diesem Sinne handelt es sich allerdings nur, wenn sie von mehreren der in § 2 Abs. 1 Satz 1 Nrn. 1 - 3 genannten Stellen gebildet wird. Eine nur vom Land oder einer Gemeinde gegründete Gesellschaft unterliegt nicht dem NDSG, sondern den Bestimmungen des BDSG, die für nicht öffentliche Stellen gelten. Dies gilt auch für Vereinigungen, an denen sowohl öffentliche Stellen als auch nicht öffentliche Stellen (natürliche Personen oder juristische Personen des privaten Rechts) beteiligt sind.

1.2

Die in § 2 Abs. 3 genannten wirtschaftlichen Unternehmen und sonstigen Einrichtungen, die überwiegend wirtschaftliche Aufgaben wahrnehmen bzw. am Wettbewerb teilnehmen, werden hinsichtlich der materiellen Datenschutzregelungen weitgehend wie private Stellen behandelt und unterliegen, soweit personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeitet werden, den Vorschriften des BDSG für nicht öffentliche Stellen. Hierzu zählen die Eigenbetriebe gem. § 108 Abs. 2 Nr. 1 NGO (z. B. Verkehrs- und Versorgungsbetriebe) und die öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden. Krankenhäuser in öffentlich-rechtlicher Trägerschaft gehören unabhängig von ihrer Zuordnung nach § 116 a Abs. 2 Satz 2 NGO zu den Einrichtungen im Sinne des § 2 Abs. 3 Satz 1 Nr. 1, die am Wettbewerb teilnehmen. Dies gilt jedoch nicht, soweit Krankenhäuser hoheitliche Aufgaben (z. B. im Rahmen von Zwangseinweisungen) wahrnehmen.

Soweit Hochschulkliniken der Patientenversorgung dienen, gehören sie zu den Einrichtungen, die am Wettbewerb teilnehmen. Gleiches gilt für die Erbringung von Leistungen gewerblicher Art (z. B. Laboruntersuchungen und gutachterliche Stellungnahmen). Hinsichtlich der übrigen von ihnen wahrzunehmenden Aufgaben,

z. B. Lehre und Forschung, unterliegen sie uneingeschränkt den Regelungen des NDSG.

Für die Verarbeitung personenbezogener Daten der Beschäftigten dieser Stellen ist ebenso wie bei den öffentlichen Stellen nach § 2 Abs. 1 Satz 1 das NDSG i.V.m. den bereichsspezifischen datenschutzrechtlichen Regelungen in den §§ 101 bis 101 i. V. m. § 261 Abs. 1 Nr. 2 NBG anwendbar, da sie nicht unmittelbar wirtschaftlichen Zwecken dient und die Daten damit nicht in Ausübung wirtschaftlicher Tätigkeit verarbeitet werden. Auch die Aufsichtsbefugnisse der oder des Landesbeauftragten für den Datenschutz ergeben sich uneingeschränkt aus dem NDSG.

1.3

Für öffentlich-rechtliche Kreditinstitute und Versicherungsanstalten sowie deren Vereinigungen enthält § 2 Abs. 4 eine spezielle Regelung. Auf diese Stellen findet abweichend von § 2 Abs. 3 nur § 24 i. d. F. vom 17.06.1993 als bereichspezifische Regelung für die Datenverarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen Anwendung (siehe Nrn. 18.1 bis 18.7 der VV NDSG vom 23.06.1994, Nds. MBl. S. 1147).

1.4

§ 2 Abs. 7 enthält eine klarstellende Regelung für das Verhältnis des NDSG zum Verwaltungsverfahrensgesetz für das Land Niedersachsen (NVwVfG). Die in § 1 Abs. 1 Satz 1 NVwVfG i.V.m. § 24 VwVfG enthaltenen Regelungen über Art und Umfang der Ermittlungen und die Regelungen in § 1 Abs. 1 Satz 1 NVwVfG i.V.m. § 26 VwVfG über die zugelassenen Beweismittel (insbesondere Einholung von Auskünften und Anhörung von Beteiligten, Zeugen sowie Beiziehung von Urkunden und Akten) werden durch die Regelungen des NDSG verdrängt, soweit personenbezogene Daten erhoben werden sollen. Auch eine Übermittlung personenbezogener Daten im Wege der Amtshilfe ist nur im Rahmen der einschränkenden Bestimmungen des NDSG, insbesondere über die Zweckbindung (§ 11 Abs. 1 i. V. mit § 10 Abs. 2), zulässig (vgl. § 5 Abs. 2 Nr. 1 VwVfG).

Die in § 29 VwVfG geregelte Akteneinsicht der Verfahrensbeteiligten besteht dagegen neben dem Recht auf Auskunft und Einsicht in Akten nach § 16. Dies gilt auch, soweit Verfahrensbeteiligte im Rahmen einer Akteneinsicht nach § 29 VwVfG personenbezogene Daten Dritter zur Kenntnis erhalten (vgl. § 13 Abs. 1 Satz 1 Nr. 2). Bereichsspezifische und damit dem NDSG vorgehende Regelungen sind insbesondere in den Bestimmungen im VwVfG über Planfeststellungsverfahren (Teil V des VwVfG) enthalten, soweit diese Regelungen die Verarbeitung personenbezogener Daten zwingend voraussetzen, z. B. durch die in § 74 Abs. 4 VwVfG vorgeschriebene Zustellung und öffentliche Auslegung des Planfeststellungsbeschlusses. Einschränkungen für die Zulässigkeit der damit verbundenen Datenübermittlung ergeben sich allerdings im Einzelfall aus dem Verhältnismäßigkeitsgrundsatz, vgl. Beschluss des Bundesverfassungsgerichts vom 24.07.1990 - BvR 1244/87 - (DVBl. S. 1041). Auch unter Berücksichtigung

des in Massenverfahren besonders gewichtigen Gesichtspunktes der Verwaltungspraktikabilität muss danach geprüft werden, inwieweit eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses notwendig voraussetzt, dass die inhaltliche Auseinandersetzung mit den geltend gemachten Einwendungen personenbezogen erfolgt und mit der Begründung veröffentlicht wird.

Zu § 3 (Begriffsbestimmungen)

2.1

Das NDSG geht von einem umfassenden Begriff der Datenverarbeitung aus. § 3 Abs. 2 umfasst daher auch jede aktenmäßige Verarbeitungsform.

Bei der Weitergabe von Daten innerhalb einer Behörde im organisatorischen Sinne handelt es sich nicht um ein Übermitteln, das nach § 3 Abs. 2 Satz 2 Nr. 4 eine Bekanntgabe an Dritte voraussetzt, sondern um ein Nutzen personenbezogener Daten. Die Zulässigkeit der behördeninternen Datenweitergabe richtet sich nach § 11 Abs. 4.

2.2

Die Pflichten des NDSG treffen die für die Datenverarbeitung verantwortliche Stelle. Da im öffentlichen Bereich die Daten verarbeitende Stelle in der Regel auch die für die Datenverarbeitung verantwortliche Stelle ist, hat der Gesetzgeber von einer Anpassung an den Wortlaut der EG-Datenschutzrichtlinie abgesehen. Die Daten verarbeitende Stelle bleibt auch bei der Beauftragung anderer Behörden und externer Dienstleister für die Einhaltung der datenschutzrechtlichen Bestimmungen während der von ihr veranlassten Verarbeitungen verantwortlich.

2.3

Das novellierte NDSG verzichtet auf die Verwendung des Dateibegriffs. Sowohl die Begriffsbestimmung der automatisierten wie der nicht automatisierten Datei entfallen. An die Stelle der Dateibeschreibung ist die Verfahrensbeschreibung getreten. Da automatisierte Dateien nur mit Hilfe von automatisierten Verarbeitungen erzeugt oder ausgewertet werden können, sind sie stets als Bestandteil einer automatisierten Verarbeitung anzusehen. Soweit in bereichsspezifischen Regelungen der Begriff der automatisierten Datei verwendet wird, finden demzufolge darauf ergänzend die Bestimmungen für die automatisierte Verarbeitung Anwendung.

Zu § 4 (Zulässigkeit der Datenverarbeitung

3.1

Soweit die Datenverarbeitung auf eine Rechtsgrundlage gestützt werden kann, widerspricht es den Zielen des NDSG, wenn von Betroffenen eine Einwilligungserklärung eingeholt wird.

3.2.

Eine wirksame Einwilligung setzt voraus, dass insbesondere der Zweck der Verarbeitung und beabsichtigte Übermittlungen Bestandteil der Einwilligungserklärung

sind. Der Umfang der Ermächtigung zur Datenverarbeitung ergibt sich in diesen Fällen grundsätzlich aus den Festlegungen in der Einwilligungserklärung. Ausnahmen hiervon sind lediglich die aus überwiegendem Allgemeininteresse vorgesehenen speziellen Vorschriften über die zweckdurchbrechende Verarbeitung erhobener oder gespeicherter Daten (§ 10).

Die Verarbeitung personenbezogener Daten nach § 4 Abs. 2 Satz 2 setzt eine bereichsspezifische gesetzliche Ermächtigung oder eine Einwilligung voraus, in der ausdrücklich die zu verarbeitenden Kategorien von Daten nach § 4 Abs. 2 Satz 2 genannt werden.

Zu § 6 (Verarbeitung personenbezogener Daten im Auftrag)

4.1

Soweit personenbezogene Daten im Rahmen der Wartung oder Fernwartung von Datenverarbeitungssysteme zwingend genutzt werden müssen, ist dies als Datenverarbeitung im Auftrag im Sinne des § 6 zulässig. Ob weitergehende Schutzvorschriften (z. B. § 203 StGB) berührt sind, ist gesondert zu prüfen.

4.2

Lässt eine öffentliche Stelle des Landes personenbezogene Daten im Auftrag von einer Stelle außerhalb des Landes Niedersachsen verarbeiten, so hat der Auftraggeber die zuständige Datenschutzkontrollbehörde zu unterrichten. Handelt es sich bei dem Auftragnehmer um eine öffentliche Stelle eines anderen Landes oder des Bundes, so ist zuständige Datenschutzkontrollbehörde die oder der jeweilige Landesdatenschutzbeauftragte bzw. die oder der Bundesbeauftragte für den Datenschutz. Handelt es sich bei dem Auftragnehmer um eine nichtöffentliche Stelle, ist die nach § 38 BDSG zuständige Aufsichtsbehörde zu unterrichten.

Im Rahmen der vertraglichen Verpflichtung nicht öffentlicher Stellen als Auftragnehmer, jederzeitige vom Auftraggeber veranlasste Kontrollen zu ermöglichen, ist auch das Prüfungsrecht der oder des Landesbeauftragten für den Datenschutz zu gewährleisten. In jedem Fall haben sich die Auftraggeber von der Beachtung der Regelungen des § 7 und der Einhaltung der erteilten Weisungen zu vergewissern.

Zu § 6 a (Mobile personenbezogene Speicher- und Verarbeitungsmedien)

5.1

Mit dem Begriff „mobile personenbezogene Speicher- und Verarbeitungsmedien“ werden nach dem heutigen Stand der Technik vor allem Chipkarten erfasst. Die Vorschrift erfasst nur solche Speicher- und Verarbeitungsmedien, auf denen personenbezogene Daten der Karteninhaberin oder des Karteninhabers verarbeitet werden; die mobilen personenbezogenen Speicher- und Verarbeitungsmedien müssen von einer öffentlichen Daten verarbeitenden Stelle ausgegeben worden sein. Nicht erfasst werden tragbare Computer (z. B. Laptop, Palmtop), die an Mitarbeiter zur Aufgabenerfüllung herausgegeben werden.

5.2

Der Pflicht, den Betroffenen die Kenntnisnahme der auf dem Medium gespeicherten Daten zu ermöglichen, wird auch genügt, wenn die für Zwecke der Verarbeitung aufgestellten Endgeräte zusätzlich eine Funktion bieten, die es der Karteninhaberin oder dem Karteninhaber ermöglicht, die auf der Karte gespeicherten personenbezogenen Daten einzusehen. Soweit die weitergehenden Rechte nach §§ 16 und 17 nicht als Funktion zur Verfügung stehen, sind Hinweise zu geben, gegenüber welcher Stelle die Betroffenen ihre Rechte geltend machen können.

5.3

Um zu verhindern, dass ein Datenaustausch ohne Kenntnis der Karteninhaberin oder des Karteninhabers erfolgt (z. B. bei berührungslosen Chipkarten), verpflichtet Abs. 3 die beteiligten Stellen, die Tatsache der Kommunikation für die betroffene Person eindeutig erkennbar zu machen (z. B. durch akustische Signale).

Zu § 7 (Technische und organisatorische Maßnahmen)

6.1

Unabhängig davon, ob personenbezogene Daten in Akten oder automatisiert verarbeitet werden, haben die öffentlichen Stellen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um eine datenschutzgerechte Verarbeitung der Daten sicherzustellen.

Die Datensicherung kann dann als wirksam angesehen werden, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Missbrauch bieten.

6.2

Von einer Novellierung der nach Abs. 2 zu treffenden Maßnahmen, um diese den veränderten technischen Begrifflichkeiten anzupassen, hat der Gesetzgeber Abstand genommen, weil eine entsprechende Neuregelung auch auf Bundesebene erst im Rahmen einer vom BMI beabsichtigten grundlegenden Novellierung des BDSG erfolgen soll und für die Zwischenzeit keine neuen Begriffe eingeführt werden sollten, die bereits in Kürze wieder geändert werden müssten. Neu ist die Regelung nach Nr. 8, mit der die Daten verarbeitende Stelle einer Forderung der EG-Datenschutzrichtlinie entsprechend nunmehr auch gesetzlich verpflichtet wird, die Verfügbarkeit der personenbezogenen Daten zu gewährleisten.

Das Datensicherungskonzept ist regelmäßig zu überprüfen und dem Stand der Technik anzupassen. Dem jeweiligen Stand der Technik entsprechen fortschrittliche Maßnahmen, die die praktische Eignung zur Sicherstellung einer datenschutzgerechten Verarbeitung personenbezogener Daten gesichert erscheinen lassen, insbesondere mit Erfolg erprobt worden sind. Bei der Auswahl technischer Maßnahmen sollten grundsätzlich sicherheitsüberprüfte und zertifizierte Produkte bevorzugt werden. Einen aktuellen Nachweis über zertifizierte Produkte führt das

Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 183, 53133 Bonn.

6.3

Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken in sich tragen, sind vor ihrer Einführung einer Vorabprüfung (Technikfolgenabschätzung) durch die Beauftragte oder den Beauftragten für den Datenschutz zu unterziehen, um festzustellen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können. Personenbezogene Daten, deren automatisierte Verarbeitung besondere Risiken für die Rechte der Betroffenen mit sich bringen, sind solche, deren Missbrauch oder Verlust Existenz, Leben oder Freiheit der Betroffenen gefährden oder sie in ihrer gesellschaftlichen Stellung erheblich beeinträchtigen würden. Als neu sind Technologien einzustufen, die erstmals im Anwendungsbereich des NDSG zum Einsatz kommen und bei denen noch nicht abschätzbar ist, ob die mit der Verarbeitung verbundenen Risiken für die Rechte der Betroffenen mit Maßnahmen nach § 7 Abs. 2 beherrscht werden können.

Die Ergebnisse der Technikfolgenabschätzung sind schriftlich zu dokumentieren. Dabei sind den denkbaren Gefährdungen die möglichen Sicherungs- und Vorbeugungsmaßnahmen gegenüberzustellen und verbleibende Gefahren für die Rechte der Betroffenen darzustellen und zu bewerten. Verfahrensalternativen zur angestrebten Lösung sind aufzuzeigen.

6.4

Mit § 7 Abs. 4 wird der Grundsatz der Datensparsamkeit und -vermeidung eingeführt. Die Daten verarbeitenden Stellen werden verpflichtet, bei der Auswahl und dem Einsatz von automatisierten Verfahren das Ziel zu beachten, keine oder so wenig wie möglich personenbezogene Daten zu verarbeiten. Danach ist bereits im Vorfeld bei Entwicklung und Auswahl von Datenverarbeitungssystemen darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden müssen. Es gibt damit ein übergreifendes Gestaltungsprinzip vor, das aus dem Tele- und Medienrecht übernommen worden ist und das Entstehen von Daten mit Personenbezug oder Personenbeziehbarkeit von vornherein ausschließen oder auf ein Minimum beschränken will. Dieses Prinzip ist Bestandteil eines neuen Ansatzes, der über einen Systemdatenschutz eine Reduzierung der Risiken für die informationelle Selbstbestimmung erreichen will. Auswirkungen hat es zum Beispiel hinsichtlich der Verarbeitung von personenbezogenen Daten der Beschäftigten, soweit diese benötigt werden für Zwecke der Dokumentation der Kommunikation (E-Mail-Adresse), der Protokollierung von Intra- und Internetnutzung sowie zur Überwachung der Nutzung der Datenverarbeitungsanlagen. Soweit zur Vermeidung von Missbräuchen oder zur Abwehr unzulässiger Zugriffe und Nutzungen eine Protokollierung notwendig ist, sind Systeme zu verwenden, die keine oder nur in geringem Umfang personenbezogene Daten benötigen.

Zu § 8 (Verfahrensbeschreibung)

7.

An die Stelle der Dateibeschreibung tritt die Verfahrensbeschreibung, die die aus der Anlage 1 ersichtlichen Punkte enthalten muss. Die Beschreibung erfolgt für das Verfahren und nicht für einzelne Dateien oder Verarbeitungsvorgänge. Soweit in bereichspezifischen Vorschriften die Beschreibung einer automatisierten Datei gefordert ist, finden die Regelungen zur Verfahrensbeschreibung Anwendung (vgl. 2.3).

Verfahren zur Speicherung personenbezogener Daten zu einem anderen Zweck als der inhaltlichen Auswertung, für die keine Beschreibung zu erstellen sind, sind z. B. solche, die ausschließlich Zwecken der Datenschutzkontrolle, der Datensicherung oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen und bei denen nach der verarbeitungstechnischen Nutzung die personenbezogenen Daten gelöscht oder überschrieben werden. Als vorübergehend ist eine Speicherung anzusehen, wenn die Daten innerhalb von 3 Monaten nach ihrer Erstellung gelöscht werden.

Nicht unter die Beschreibungspflicht fallen Register nach § 8 a Abs. 4. Nach der Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten nach § 8 a, entfällt die Beschreibungspflicht für die Tätigkeit der Notarinnen und Notare sowie für die Verfahren zur Textverarbeitung einschließlich der Übermittlung elektronischer Dokumente über Telekommunikationsdienste an die Empfängerinnen und Empfänger.

Zu § 8 a (Behördliche Datenschutzbeauftragte)

8.1

Grundsätzlich haben alle öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten, Datenschutzbeauftragte zu bestellen, unabhängig von der Zahl der damit befassten Mitarbeiterinnen und Mitarbeiter. Außerhalb von Rechenzentren liegt eine automatisierte Datenverarbeitung vor, soweit Terminals zur Datenfernverarbeitung, Personalcomputer, Mehrplatzsysteme oder vernetzte Systeme zur Aufgabenerledigung eingesetzt werden.

Die Bestellung der Beauftragten oder des Beauftragten für den Datenschutz erfolgt durch die Leiterin oder den Leiter der Behörde oder sonstigen öffentlichen Stelle, bei der die Datenverarbeitungsanlagen oder die Datenendgeräte betrieben werden. Bestellt werden können auch Personen, die nicht der Daten verarbeitenden Stelle angehören, insbesondere können z. B. Gemeinden die Aufgaben eines oder einer Beauftragten für den Datenschutz Angehörigen der Kommunalen Datenzentralen übertragen. Es ist auch möglich, gemeinsam eine oder einen Beauftragten für den Datenschutz zu bestellen. Werden bei einer Stelle Sozialdaten verarbeitet, gilt § 8 a in Verbindung mit § 81 Abs. 4 Satz 4 SGB X.

Die Bestellung und ggf. auch Abberufung unterliegt gemäß § 67 Abs. 1 Nr. 9 NPersVG der Mitbestimmung des Personalrats.

8.2

Die oder der Beauftragte für den Datenschutz unterstützt die öffentliche Stelle bei der Sicherstellung des Datenschutzes und wirkt auf die Einhaltung der datenschutzrechtlichen Vorschriften hin.

Mit der Funktion sollen nicht Personen betraut werden, die dadurch in Interessenkonflikte geraten können, die über das unvermeidliche Maß hinausgehen; das wird i. d. R. der Fall sein, wenn z. B. die Leiterin oder der Leiter von Rechenzentren oder Bedienstete der Systemverwaltung oder deren unmittelbare Vorgesetzten zur Beauftragten oder zum Beauftragten für den Datenschutz bestellt werden sollen. Die oder der Beauftragte für den Datenschutz hat vorrangig die Aufgabe, bei der Ausgestaltung der technischen und organisatorischen Maßnahmen nach § 7 zu beraten und auf die Durchführung der Maßnahmen sowie der Aufgaben nach § 8 hinzuwirken. Dabei hat sie oder er im Bereich der automatisierten Datenverarbeitung insbesondere

- auf der Grundlage des § 7 Abs. 2 zu prüfen, welche Maßnahmen zur Datensicherung erforderlich und angemessen sind,
- beim Erlass von Dienstanweisungen über getroffene bzw. zu treffende Datensicherungsmaßnahmen mitzuwirken,
- die Behördenleitung und die Beschäftigten aufgrund ihrer bzw. seiner Sachkenntnis in Fragen des Datenschutzes und der Datensicherung zu beraten und
- gegebenenfalls bei der Erledigung von Auskunftsbegehren nach § 16 mitzuwirken.

Damit die Beauftragten für den Datenschutz frühzeitig auf eine sachgerechte Ausgestaltung der Maßnahmen nach § 7 hinwirken können, sind sie bereits über geplante Verfahren zur automatisierten Verarbeitung personenbezogener Daten zu unterrichten.

8.3

Die Beauftragten für den Datenschutz haben auf Antrag, ohne dass es hierfür besonderer Voraussetzungen bedarf, jedermann die Verfahrensbeschreibungen, die ihnen von den Daten verarbeitenden Stellen zur Verfügung zu stellen sind, zugänglich zu machen. Über die Art und Form, z. B. Einsichtnahme oder kostenpflichtige Übersendung von Kopien, entscheiden die Beauftragten für den Datenschutz. Zulässig ist auch eine Veröffentlichung im Internet, wenn sichergestellt ist, dass sich die Informationen auf die Angaben zu Nr. 1 bis 6 der Verfahrensbeschreibungen (Seiten 1 - 3 der Anlage 1 - ohne den behördeninternen Teil) beschränken und Informationen, die zu einer Beeinträchtigung der Verfahrenssicherheit führen könnten, nicht offenbart werden. Gänzlich ausgenommen von dieser Verpflichtung sind Beschreibungen, wenn die Verarbeitungen der Erfüllung von Aufgaben nach dem Nds. Verfassungsschutzgesetz oder polizeilicher Aufgaben nach dem Nds. Gefahrenabwehrgesetz oder zum Zweck der Strafverfolgung erfolgen.

Den Beauftragten für den Datenschutz obliegt die Vorabprüfung von Verfahren nach § 7 Abs. 3. Für die Durchführung hierfür notwendiger Erhebungen und Prüfungen kann er sich der Unterstützung der Daten verarbeitenden Stelle bedienen. Bei behörden- oder ressortübergreifenden Verfahren liegt die Zuständigkeit zur Vorabprüfung bei der oder dem Beauftragten für den Datenschutz der öffentlichen Stelle, die für die Einführung des Verfahrens verantwortlich ist.

8.4

Keine Beauftragten für den Datenschutz sind zu bestellen für öffentliche Stellen, die lediglich Register führen, die zur Information der Öffentlichkeit bestimmt sind und entweder jedermann oder allen Personen, die ein berechtigtes Interesse geltend machen, offen stehen. Nach der Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten nach § 8 a, entfällt die Pflicht zur Bestellung von Beauftragten für den Datenschutz für die Tätigkeit der Notarinnen und Notare sowie für die Verfahren zur Textverarbeitung einschließlich der Übermittlung elektronischer Dokumente über Telekommunikationsdienste an die Empfängerinnen und Empfänger.

Zu § 9 (Erhebung)

9.1

§ 9 Abs. 1 Satz 3 nennt verschiedene Fälle, in denen Daten ohne Kenntnis der Betroffenen erhoben werden dürfen. Dazu gehört auch die Erhebung von Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen gegenüber der Daten verarbeitenden Stelle, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen. Bei der Datenerhebung zu Ausbildungs- und Prüfungszwecken ist auch der in § 10 Abs. 3 Satz 2 enthaltende Gedanke (offensichtliches Überwiegen der berechtigten Interessen der Betroffenen an der Geheimhaltung der Daten) zu berücksichtigen.

Der Ausnahmetatbestand für die Datenerhebung aus allgemein zugänglichen Quellen (§ 9 Abs. 1 Satz 3 Nr. 5) ist mit der Einschränkung versehen, dass schutzwürdige Interessen der Betroffenen nicht offensichtlich entgegenstehen dürfen. Damit soll berücksichtigt werden, dass in Einzelfällen bei sensiblen persönlichen Daten die Rechtfertigung der Datenverarbeitung allein mit einer womöglich schon lange zurückliegenden - und vielleicht ihrerseits problematischen - Veröffentlichung bedenklich sein kann, wenn damit der Schutz der personenbezogenen Daten auf Dauer durchbrochen wird.

9.2

Für die in § 9 Abs. 2 geregelten Aufklärungs- und Unterrichtungspflichten bei der Datenerhebung bei Betroffenen ist anders als in § 4 Abs. 2 keine Schriftform vorgeschrieben. Gleichwohl sollte die Aufklärung in der Regel schriftlich erfolgen, um die Betroffenen in die Lage zu versetzen, ihre Rechte wahrnehmen zu können. Soweit Daten schriftlich erhoben werden, ist auch die Aufklärung in schriftlicher Form vorzunehmen. Eine besondere Unterrichtung über den Verwendungszweck

ist nach § 9 Abs. 2 dann entbehrlich, wenn sich dieser aus den Gesamtumständen der Datenerhebung für Betroffene eindeutig erkennbar ergibt. Ein Verstoß gegen die Aufklärungspflichten macht die Datenerhebung nicht ohne weiteres unwirksam und hindert die weitere Datenverarbeitung damit grundsätzlich nicht. Anders ist die Rechtslage, wenn der Hinweis auf die Freiwilligkeit unterlassen wurde. In diesem Fall dürfen die erhobenen Daten nicht gespeichert werden, sie sind vielmehr von Amts wegen zu löschen (§ 17 Abs. 2 Nr. 1).

Im Rahmen des Hausrechts ist eine Beobachtung mit optisch-elektronischen Einrichtungen (Videoüberwachung) z. B. zur Sicherung von Dienstgebäuden zulässig, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen dem entgegen stehen. Der Umstand der Beobachtung und der Zweck muss für die Betroffenen erkennbar sein (ggf. durch Anbringen von Hinweisschildern). Die dabei erhobenen Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind, oder schutzwürdige Interessen der Betroffenen einer Speicherung entgegenstehen (§ 17 Abs. 2 Nr. 2).

Für öffentliche Stellen im Sinne von § 2 Abs. 3 richtet sich die Zulässigkeit der Videoüberwachung nach § 6 b BDSG[1)].

Als spezielle bereichspezifische, dem NDSG vorgehende Regelung ist § 32 Abs. 3 NGefAG[1)] anzusehen, der die Polizei und die Verwaltungsbehörden der Gefahrenabwehr ermächtigt, öffentlich zugängliche Orte mittels Bildübertragung offen zu beobachten, wenn dies zur Erfüllung von Aufgaben nach § 1 Abs. 1 NGefAG[1)] erforderlich ist.

[1)] Hinweis der Redaktion:

Für Änderungen der VV NDSG ist MI zuständig. Einige Regelungen in den VV NDSG sind überholt:

- Vgl. zwischenzeitlich in Kraft getretene Regelung zur Videoüberwachung in § 25 a NDSG
- Im letzten Absatz sind die beiden Worte „NGefAG“ jeweils durch das Wort „Nds. SOG“ zu ersetzen.

Zu § 10 (Speicherung, Veränderung, Nutzung; Zweckbindung)

10.1

Nach § 10 Abs. 1 dürfen personenbezogene Daten nur für die Zwecke verarbeitet werden, für die sie erhoben oder - falls keine Erhebung vorausgegangen ist - erstmals gespeichert worden sind. Aufgrund dieses Zweckbindungsprinzips kommt der Festlegung des Verarbeitungszwecks für die Zulässigkeit der weiteren Verarbeitung der Daten eine zentrale Bedeutung zu (vgl. § 10 Abs. 2).

Werden Daten bei den Betroffenen erhoben, wird der Zweck durch die Aufklärung nach § 9 Abs. 2 Satz 1 begrenzt. Bei entsprechender Aufklärung können Daten auch gleichzeitig für unterschiedliche Zwecke erhoben werden.

Werden Daten in Ausführung einer Rechtsvorschrift verarbeitet, ergibt sich aus ihr auch der Zweck der Datenverarbeitung. Soweit in der Rechtsvorschrift keine besonderen Regelungen für die Verarbeitung personenbezogener Daten enthalten sind, kann in der Regel davon ausgegangen werden, dass es sich bei der Ausführung der Rechtsvorschrift insgesamt um einen Zweck und nicht verschiedene Zwecke im Sinne des § 10 Abs. 1 und 2 handelt.

10.2

§ 10 Abs. 2 Satz 2 enthält eine Sonderregelung für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind.

Berufsgeheimnissen in diesem Sinne unterliegen die Angehörigen der in § 203 Abs. 1 Strafgesetzbuch genannten Berufe. Zu den besonderen Amtsgeheimnissen gehören alle Geheimnisse, die aufgrund besonderer Rechtsvorschriften über das allgemeine Amtsgeheimnis, das seinen Ausdruck in § 30 Verwaltungsverfahrensgesetz, den dienst- und arbeitsrechtlichen Verschwiegenheitspflichten und in § 5 gefunden hat, hinausgehen. Hierzu gehören z. B. das Statistikgeheimnis, das Steuergeheimnis, das Post- und das Fernmeldegeheimnis.

10.3

Die Bearbeitung von Personalakten im Rahmen praxisgerechter Ausbildung hat in Abwägung mit den berechtigten Interessen der Betroffenen an der Geheimhaltung ihrer Daten zu erfolgen. Dabei sind folgende Punkte zu berücksichtigen:

Soweit möglich, ist es zu vermeiden, dass Auszubildende Personalakten von Bediensteten der Beschäftigungsbehörde bearbeiten, bei der die Auszubildenden später verbleiben. Statt dessen kommt z. B. die Ausbildung an Vorgängen nachgeordneter Bereiche in Betracht, deren Bedienstete den Auszubildenden nicht persönlich bekannt sind. Wenn die Ausbildungspläne auch Stationen in anderen Behörden vorsehen, könnte eine Zuweisung in deren Personalstellen erfolgen.

Der Personalstellenleitung und der Ausbilderin oder dem Ausbilder obliegt es, ausbildungsfördernde Einzelfälle gezielt zur Bearbeitung zu übertragen; dabei ist darauf zu achten, dass besonders sensible Personalvorgänge nicht herangezogen werden.

Es sind nur die bearbeitungsrelevanten Personalakten bzw. Personalaktenteile zur Verfügung zu stellen; eine generelle Zugriffsmöglichkeit auf die Personalakten ist auszuschließen, siehe auch Nr. 8.1 der VV zu § 101 NBG (Nds. MBl. 1993 S. 93).

Zu § 10 a (Automatisierte Einzelentscheidung)

11.1

Mit § 10 a trifft der Gesetzgeber in Umsetzung der EG-Datenschutzrichtlinie eine grundsätzliche Wertentscheidung, nach der Betroffene nicht einer Entscheidung unterworfen werden sollen, die ausschließlich auf einer automatisierten Bewertung

einzelner Persönlichkeitsmerkmale wie z. B. Zuverlässigkeit oder berufliche Leistungsfähigkeit beruht.

11.2

Damit Betroffene ihre Rechte wirksam ausüben können, erstreckt sich ihr Auskunftsanspruch auch auf den logischen Aufbau bzw. Art und Struktur der der automatisierten Einzelentscheidung zugrunde liegenden automatisierten Verarbeitung. Die Begriffe logischer Aufbau bzw. Art und Struktur der automatisierten Verarbeitung (vgl. § 16) sind inhaltsgleich und sollen deutlich machen, dass die Betroffen darüber informiert werden müssen, nach welchen Entscheidungskriterien und Bewertungsmusterns automatisierte Einzelentscheidungen ergehen.

Zu § 11 (Datenübermittlung innerhalb des öffentlichen Bereichs)

12.

Für die Übermittlung personenbezogener Daten durch eine Weitergabe von Akten sieht § 11 Abs. 2 Verfahrenserleichterungen vor. Die datenverarbeitende Stelle wird ihre Aktenführung allerdings so einrichten, dass eine Aktentrennung möglichst erreicht werden kann (z. B. vergleichbar der Regelung in Nr. 4.3 der VV zu § 101 NBG für die Personalaktenverwaltung). Ob ein unvertretbarer Aufwand vorliegt, kann in der Regel nur im Einzelfall entschieden werden. Die in § 11 Abs. 2 enthaltene Regelung gilt nicht für die automatisierte Verarbeitung personenbezogener Daten.

Zu § 12 (Automatisiertes Abrufverfahren)

13.1

Die Regelungen in § 12 gelten sowohl für bereits bestehende wie auch für geplante automatisierte Abrufverfahren unabhängig von der eingesetzten Technologie. So werden auch Abrufverfahren, die im Rahmen eines Internetangebots eingerichtet werden, mit erfasst. Die Regelungen finden jedoch keine Anwendung für die Einrichtung entsprechender Verfahren innerhalb einer öffentlichen Stelle. Hierbei ist anders als bei der Einrichtung automatisierter Abrufverfahren im Anwendungsbereich des SGB vom organisatorischen Behördenbegriff auszugehen. Geplante automatisierte Abrufverfahren sind der jeweils zuständigen obersten Landesbehörde mitzuteilen.

13.2

Soweit entsprechende Verfahren im Rahmen der Wahrnehmung von Aufgaben des übertragenen Wirkungskreises von Gemeinden, Landkreise und sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts eingerichtet werden sollen, ist hierfür ebenfalls eine Verordnung erforderlich.

Sollen automatisierte Abrufverfahren zur Wahrnehmung von Aufgaben des eigenen Wirkungskreises eingerichtet werden, können diese nach § 12 Abs. 1 in Ver-

bindung mit der satzungsbegründenden Rechtsvorschrift (z. B. § 6 NGO, § 5 NLO) durch Satzung zugelassen werden. Dabei sind die in § 12 Abs. 2 Sätze 3 und 4 enthaltenen Vorgaben zu berücksichtigen. Nach § 22 Abs. 1 ist die oder der Landesbeauftragte für den Datenschutz vor dem Erlass einer solchen Satzung anzuhören .

Zu § 13 (Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs)

14.

Ein rechtliches Interesse nach § 13 Abs. 1 Satz 1 Nr. 2 liegt vor, wenn die Kenntnis der Daten für den Empfänger zur Verfolgung von Rechtsansprüchen oder Abwehr entsprechender Forderungen erforderlich ist. Das berechtigte Interesse im Sinne des § 13 Abs. 1 Satz 1 Nr. 3 umfasst darüber hinaus jedes private, ideelle oder vermögenswerte Interesse, das von der Rechtsordnung als schutzwürdig anerkannt wird.

Zu § 14 (Übermittlung an Personen oder Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums)

15.1

Auch wenn die in § 14 Satz 1 genannten Voraussetzungen nicht vorliegen, ist eine Übermittlung personenbezogener Daten an Personen und Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums unter den gleichen Voraussetzungen zulässig, die bei einer Datenübermittlung an Personen oder Stellen innerhalb des Europäischen Wirtschaftsraums (Inland, EU-Mitgliedsstaaten und die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, z. Z. Norwegen, Island und Liechtenstein) zu beachten sind (vgl. § 11 Abs. 1 und § 13 Abs. 1), sofern im Empfängerland gleichwertige Datenschutzregelungen gelten. Als gleichwertig können Regelungen zur Gewährleistung eines Datenschutzstandards anerkannt werden, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (BGBl. II S. 538) ergibt. Dies gilt für Kanada, Israel, Ungarn, die Schweiz sowie die Vereinigten Staaten von Amerika. Im Hinblick auf den Umfang der Ausnahmen nach Abs. 2 wird in der Praxis eine Prüfung, ob im Empfängerland gleichwertige Datenschutzbestimmungen gelten, nur in Ausnahmefällen erforderlich werden. Soweit im Einzelfall Zweifel bestehen, ob im Empfängerland gleichwertige Datenschutzregelungen gelten, ist dem Nds. Innenministerium zu berichten.

Ausländische Personen und nichtöffentliche Stellen sind entsprechend § 13 Abs. 2 zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie ihnen übermittelt worden sind.

15.2

Unabhängig von dem Vorliegen gleichwertiger Datenschutzbestimmungen dürfen personenbezogene Daten übermittelt werden, soweit die Ausnahmen des Absatzes 2 vorliegen. Bei öffentlichen Registern muss in den Fällen der Nr. 3 b) die ausländische Person oder Stelle das berechtigte Interesse an der Einsichtnahme glaubhaft machen.

Zu § 15 (Übermittlung an Stellen öffentlich-rechtlicher Religionsgesellschaften)

16.1

§ 15 enthält eine besondere Regelung für die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften. Die Übermittlung personenbezogener Daten an privat-rechtliche Religionsgesellschaften ist unter den in § 13 genannten Voraussetzungen zulässig. Privat-rechtlich organisierte Einrichtungen und Werke öffentlich-rechtlicher Religionsgesellschaften gehören nicht zu den in § 15 genannten Stellen; für die Übermittlung von Daten an diese gilt § 13.

Die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften nach § 15 Satz 1 Nrn. 3 bis 5 ist nur zulässig, wenn sichergestellt ist, dass bei den Empfängern ausreichende Datenschutzmaßnahmen getroffen sind. Bei den nachfolgend aufgeführten öffentlich-rechtlichen Religionsgesellschaften ist davon auszugehen, dass ausreichende Datenschutzmaßnahmen, insbesondere Regelungen zur Zweckbindung, getroffen sind. Im übrigen sind die Voraussetzungen im Einzelfall zu prüfen.

Evangelische Landeskirchen

Evangelisch-lutherische Landeskirche in Braunschweig,

Evangelisch-lutherische Landeskirche Hannovers,

Evangelisch-Lutherische Kirche in Oldenburg,

Evangelisch-Lutherische Landeskirche Schaumburg-Lippe,

Evangelisch-reformierte Kirche (Synode ev.-ref. Kirchen in Bayern und Nordwestdeutschland),

auf niedersächsischem Gebiet liegende Teile von Kirchengemeinden der Nordelbischen Evangelisch-lutherische Kirche,

auf niedersächsischem Gebiet liegende Teile von Kirchengemeinden der Bremischen ev. Kirche,

auf niedersächsischem Gebiet liegende Teile von Kirchengemeinden der ev. Kirche von Westfalen.

Evangelisch reformierte Gemeinden

Evangelisch reformierte Gemeinden außerhalb der Landeskirchen

Evangelisch-reformierte Gemeinde in Braunschweig,

Evangelisch-reformierte Kirche in Bückeburg,

Evangelisch-reformierte Gemeinde in Göttingen,

Evangelisch-reformierte Kirche in Stadthagen.

Römisch-katholische Kirche

Diözesen Hildesheim und Osnabrück, soweit sie zum Bereich des Landes Niedersachsen gehören,

der oldenburgische Teil der Diözese Münster,

die Kirchengemeinde Bad Pyrmont der Erzdiözese Paderborn.

Andere

Katholische Pfarrgemeinde der Alt-Katholiken Hannover-Niedersachsen

Landesverband der Jüdischen Gemeinden von Niedersachsen

16.2

Soweit die Betroffenen in die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften eingewilligt haben oder eine bereichsspezifische Rechtsvorschrift die Datenübermittlung vorsieht, ist ebenfalls nicht zu prüfen, ob sichergestellt ist, dass bei diesen Stellen ausreichende Datenschutzmaßnahmen getroffen sind. Die Datenübermittlung ist dann bereits nach § 4 Abs. 1 Nr. 2 bzw. § 4 Abs. 1 Nr. 1 2. Alt. zulässig.

Zu § 16 (Auskunft, Einsicht in Akten)

17.1

Eine Gefährdung der ordnungsgemäßen Wahrnehmung der sonstigen Aufgaben einer öffentlichen Stelle (§ 16 Abs. 4 Nr. 1) kann nur befristet einem Auskunfts- oder Einsichtsverlangen entgegengehalten werden. In derartigen Fällen ist zu prüfen, ob nicht auch durch Teilauskünfte dem Verlangen zunächst Rechnung getragen werden kann. Auskunft ist auch zu darüber zu erteilen, ob die Daten verarbeitende Stelle personenbezogene Daten im Auftrage von anderen Stellen verarbeiten lässt. Soweit dies geschieht, erstreckt sich der Auskunftsanspruch auch auf die Nennung der Auftragnehmer.

Ob die Auskunft oder Akteneinsicht die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde, wird von der Daten verarbeitenden Stelle nicht immer überblickt werden können. In Zweifelsfällen sind Stellungnahmen der zuständigen Behörden der Gefahrenabwehr, der Strafverfolgung oder des Verfassungsschutzes einzuholen.

17.2

Die Ablehnung eines Auskunfts- oder Akteneinsichtsverlangens ist zu begründen, soweit nicht der Ausnahmegrund des § 16 Abs. 5 Satz 1 vorliegt.

17.3

Für eine Auskunft oder Akteneinsicht sind weder Gebühren noch Auslagen zu erheben. Von der Kostenfreiheit nicht erfasst sind Leistungen, die über eine Aus-

kunft oder Akteneinsicht hinausgehen und die nach allgemeinem Kostenrecht (VwKostG i.V.m. NVwKostG, AllGO, Anlage 2) gebühren- bzw. erstattungspflichtig sind, wie z. B. die Anfertigung von Ablichtungen, Entscheidungen im förmlichen Rechtsbehelfsverfahren.

Zu § 17 (Berichtigung, Löschung und Sperrung)

18.1

Bevor personenbezogene Daten nach § 17 Abs. 2 Satz 1 Nr. 2 gelöscht werden, haben die öffentlichen Stellen des Landes die Akten oder sonstigen Datenträger dem zuständigen Staatsarchiv zur Übernahme anzubieten (vgl. § 3 des Niedersächsisches Archivgesetzes). Auf die speziellen Anbietungspflichten nach § 3 Abs. 6 Satz 1 und § 7 Abs. 3 des Niedersächsischen Archivgesetzes wird hingewiesen.

Soweit für die Aufbewahrung von Akten nicht bereichsspezifische Aufbewahrungsfristen vorgeschrieben sind, ist die Löschung nach § 17 Abs. 2 Satz 1 Nr. 2 durchzuführen, wenn die in der Niedersächsischen Aktenordnung oder dem Niedersächsischen Aktenplan genannten Aufbewahrungsfristen abgelaufen sind.

Bei der Aussonderung von Akten oder sonstigen Datenträgern ist darauf zu achten, dass die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um personenbezogene Daten insbesondere vor dem Zugriff Unbefugter zu schützen (§ 7 Abs. 1 und 4). Auch eine Zwischenlagerung des ausgesonderten Schriftguts bis zur Vernichtung muss diesen Anforderungen entsprechen.

Zur Vernichtung von Schriftgut kann eine öffentliche Stelle auch eine andere Behörde beauftragen, die einen Aktenvernichter besitzt. Sowohl bei der Beauftragung einer anderen öffentlichen Stelle wie auch eines privaten Unternehmens handelt es sich um einen Auftrag i. S. des § 6. Der Auftrag zur Löschung personenbezogener Daten, die Weisungen zu technischen und organisatorischen Maßnahmen sowie die Zulassung von Unterauftragsverhältnissen sind daher nach § 6 Abs. 2 Satz 2 schriftlich festzuhalten. Das Muster eines Vertrages über die Vernichtung von Altpapier durch einen Privatunternehmer ist als Anlage 2 beigefügt.

Für den Auftrag zur Vernichtung von Schriftgut mit Sozialdaten enthält § 80 SGB X eine bereichsspezifische Regelung.

18.2

Eine Unterrichtungspflicht gemäß § 17 Abs. 4 besteht nach dem Sinn der Regelung nicht, wenn die Daten gelöscht werden, weil ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist (§ 17 Abs. 2 Satz 1 Nr. 2).

Zu § 17 a (Widerspruchsrecht)

19.

Mit § 17 a wird den Betroffenen das Recht eingeräumt, einer rechtmäßigen Datenverarbeitung (§ 3 Abs. 2 Satz 1) zu widersprechen, soweit persönliche schutzwürdige Interessen einer Verarbeitung entgegenstehen und diese das Interesse der öffentliche Stelle an der Verarbeitung der Daten überwiegen. Ausgenommen sind hier lediglich Verarbeitungen, die aufgrund gesetzlicher Vorschriften von der Daten verarbeitenden Stelle verpflichtend durchzuführen sind.

Zu § 18 (Schadensersatz)

20.

§ 18 sieht für die Verarbeitung personenbezogener Daten eine Gefährdungshaftung vor. Soweit die Daten nicht automatisiert verarbeitet werden, trifft die öffentliche Stelle die Ersatzpflicht nicht, wenn sie nachweist, dass die Unzulässigkeit der Datenverarbeitung nicht von ihr zu vertreten ist (Umkehr der Beweislast). Dem Betroffenen obliegt der Nachweis der rechtswidrigen Verarbeitung und der Schadensverursachung.

Zu § 19 (Anrufung der oder des Landesbeauftragten)

21.

Wird einem Hinweis einer oder eines Bediensteten auf einen Verstoß gegen datenschutzrechtliche Vorschriften nicht abgeholfen, so kann sich die oder der Bedienstete nach § 19 Abs. 2 ohne Einhaltung des Dienstweges an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz wenden.

Zu § 22 (Aufgaben, Rechte und Pflichten der oder des Landesbeauftragten)

22.

In folgenden Fällen ist die oder der Landesbeauftragte zu beteiligen:

- Unterrichtung über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme (§ 22 Abs. 2),
- Zulassung automatisierter Abrufverfahren nach § 12 (§ 12 Abs. 2 Satz 5),
- bei der Einrichtung automatisierter Dateien für Aufgaben nach dem NVerfSchG (§ 12 NVerfSchG) oder polizeilicher Aufgaben nach dem NGefAG (§ 46 NGefAG)[1)] durch Übersendung einer Ausfertigung der nach § 8 zu erstellenden Beschreibung (§ 22 Abs. 5),
- Anzeige der Übermittlung personenbezogener Daten an Personen oder sonstige nicht öffentliche Stellen sowie öffentlichen Stellen außerhalb des Geltungsbereichs des NDSG für Forschungsvorhaben (§ 25 Abs. 7 Satz 2),
- bei der Ausarbeitung von Gesetzentwürfen sowie beim Erlass von Verordnungen und Verwaltungsvorschriften des Landes, die Regelungen zum Recht auf

informationelle Selbstbestimmung zum Gegenstand haben, ist die oder der Landesbeauftragte anzuhören,

- Unterrichtung über Gesetzesvorhaben (Referentenentwürfe) und den beabsichtigten Erlass von Verordnungen und Verwaltungsvorschriften des Bundes, soweit Regelungen über die Verarbeitung personenbezogener Daten vorgesehen sind und Stellen des Landes an der Erarbeitung entsprechender Entwürfe beteiligt werden.

Die Unterrichtungspflichten entbinden die datenverarbeitenden Stellen nicht von ihrer Verantwortung für die datenschutzrechtliche Zulässigkeit der Maßnahmen. Diese ist in jedem Fall von den öffentlichen Stellen in eigener Zuständigkeit zu prüfen.

[1)] Hinweis der Redaktion:

Für Änderungen der VV NDSG ist MI zuständig. Einige Regelungen in den VV NDSG sind überholt: Beim dritten Spiegelstrich sind die beiden Worte „NGefAG“ jeweils durch das Wort „Nds. SOG“ zu ersetzen.

Zu § 25 (Verarbeitung personenbezogener Daten für Forschungsvorhaben)

23.1

Die in § 25 enthaltene bereichsspezifische Regelung für die Verarbeitung personenbezogener Daten für Forschungsvorhaben geht Regelungen für die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen vor, so dass diese Daten im Rahmen der in § 25 festgelegten Voraussetzungen für Forschungsvorhaben verarbeitet werden dürfen.

23.2

§ 25 Abs. 2 lässt unter den dort genannten Voraussetzungen abweichend von § 10 Abs. 2 die Weiterverarbeitung der schon von öffentlichen Stellen des Landes gespeicherten personenbezogenen Daten für wissenschaftliche Forschungsvorhaben zu.

Die in § 25 Abs. 2 Satz 1 Nr. 3 vorgeschriebene Abwägung zwischen den schutzwürdigen Interessen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens ist von der öffentlichen Stelle, die das Forschungsvorhaben durchführt, vorzunehmen.

Wird das Forschungsvorhaben von einer Privatperson, einer sonstigen nichtöffentlichen Stelle oder einer öffentlichen Stelle, die nicht in den Anwendungsbereich des NDSG fällt (z. B. eine öffentliche Stelle des Bundes oder eines anderen Bundeslandes), durchgeführt, ist die Abwägung nach § 25 Abs. 2 Satz 1 Nr. 3 von der übermittelnden Stelle vorzunehmen. Ergänzend hierzu sind die Empfänger in diesen Fällen nach § 25 Abs. 7 zu verpflichten, die Daten nur für das von ihnen bezeichnete Forschungsvorhaben und nach Maßgabe der Absätze 3 bis 5 zu verarbeiten.

23.3

§ 25 Abs. 3 enthält eine besondere Zweckbindungsregelung, die den allgemeinen Zweckbindungsregelungen in § 10 Abs. 1 und 2 vorgeht. Eine Verarbeitung der für ein Forschungsvorhaben gespeicherten oder übermittelten Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen ist jedoch zulässig, da hierin keine zweckändernde Verarbeitung liegt (§ 10 Abs. 3 Satz 1).

23.4

Werden personenbezogene Daten an eine andere als eine öffentliche Stelle des Landes für ein Forschungsvorhaben übermittelt, ist die Übermittlung der oder dem Landesbeauftragten nach § 25 Abs. 7 S. 2 von der übermittelnden Stelle vorher so rechtzeitig anzuzeigen, dass die oder der Landesbeauftragte zu der Zulässigkeit der Datenübermittlung gegebenenfalls noch Stellung nehmen kann.

Zu § 28 (Straftaten)

24.

Mit der Änderung, dass bei der Strafbarkeit künftig auf die unbefugte Verarbeitung von „Daten die nicht allgemein zugänglich sind“ abstellt wird, soll der Rechtsprechung mehrerer Strafgerichte (z. B. BayObLG NJW 1999, S. 1727) Rechnung getragen werden, die das bisherige Merkmal „offenkundig“ für die Kfz-Halter-Datei bejaht und daher Personen, die daraus Daten weitergegeben hatten, freigesprochen haben. Auf der Grundlage dieser Rechtsauffassung konnten z. B. unbefugte Abrufe aus dem zentralen Informationssystem des Kraftfahrtbundesamtes durch einzelne öffentliche Bedienstete und die Weitergabe dieser Daten an private Stellen strafrechtlich nicht geahndet werden. Durch die Änderung des Gesetzes soll sichergestellt werden, dass bei Vorliegen der sonstigen Voraussetzungen des § 28 eine strafrechtliche Ahndung nur in denjenigen Fällen ausgeschlossen ist, in denen es sich um Daten handelt, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang aus Gründen des Persönlichkeitsschutzes rechtlich beschränkt ist.

Entsprechendes gilt für die Änderung der Regelung in § 29 (Ordnungswidrigkeiten).

Zu § 29 (Ordnungswidrigkeiten)

25.

Die Ahndung der Ordnungswidrigkeiten richtet sich bei Zuwiderhandlungen von Beschäftigten nach § 6 Nr. 9 ZustVO-OWi, im Übrigen gilt die Regelzuständigkeit.[1)]

[1)] Hinweis der Redaktion:

Für Änderungen der VV NDSG ist MI zuständig. Nr. 25 zu § 29 sollte auf Grund der zwischenzeitlich eingetretenen Änderung der ZustVO-OWi wie folgt gefasst werden:

„Die Ahndung der Ordnungswidrigkeiten richtet sich bei Zuwiderhandlungen von Beschäftigten nach § 1 Abs. 1 i. V. m. § 6 Nr. 1 ZustVO-OWi.“

Schlussbestimmungen

26.1

Den Gemeinden, Landkreisen und den der Aufsicht des Landes unterstehenden anderen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen wird empfohlen, entsprechend zu verfahren.

26.2

Der Bezugserlass wird aufgehoben.

An die

Dienststellen der Landesverwaltung,

Gemeinden, Landkreise und

sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen

Anlage 1 (Verfahrensbeschreibung - Beispiel)

Hinweis der Redaktion: Für Änderungen der VV NDSG ist MI zuständig.

Verfahrensbeschreibung gem. § 8 des Nds. Datenschutzgesetzes (NDSG)

☒ **Einzelbeschreibung der Daten verarbeitenden Stelle**

☐ **Sammelbeschreibung der Daten verarbeitenden Stelle zu gleichartigen Verfahren** — Anzahl der Verfahren: 1

☐ **Sammelbeschreibung durch Auftragnehmer (Daten verarbeitende Stelle siehe beiliegende Liste)**

☒ Ersterfassung ☐ Änderung/Ergänzung

Verfahrensbeschreibungen über automatisierte Verfahren zur Erfüllung der Aufgaben nach dem Nds.Verfassungsschutzgesetz oder polizeilicher Aufgaben nach dem Nds. Gefahrenabwehrgesetz sind in Kopie an die Landesbeauftragte/den Landesbeauftragten für den Datenschutz Niedersachsen zu senden.

1. Anzeigende Stelle

Verfahrensbeschreibung erstellt von (Adresse, Geschäftszeichen)	Telefon:	Ort, Datum:
Stadt Musterhausen, Sachgebiet Kraftfahrzeugzulassungsbehörde, Hauptstraße 1, 30000 Musterhausen, FB OE	0999/120-4561	Musterhausen, 12.09.2003
Name der oder des Datenschutzbeauftragten /Telefon Frau Schmidt, Tel. 0999/120-4575 Referat/Dezernat/Amt/Abteilung Zentrale Steuerung und Verwaltungsentwicklung	**Unterschrift** (Erstellerin/Ersteller der Verfahrensbeschreibung)	angeordnet durch Leiterin/Leiter

2. Bezeichnung des Verfahrens

Bezeichnung des Verfahrens Kraftfahrzeugzulassungswesen	
Eingesetze Programme OK.Vorfahrt der AKDB	
☒ Verknüpfungen zu anderen Verfahren oder Dateien bestehen	Bezeichnung dieser anderen Verfahren oder Dateien Microsoft Word

3. Bezeichnung der Daten verarbeitenden Stelle/ Angaben zur Auftragsdatenverarbeitung

Bezeichnung der Daten verarbeitenden Stelle (bei Sammelbeschreibung durch Auftragnehmer siehe beiliegende Liste)
Stadt Musterhausen, Fachbereich Recht und Ordnung, Sachgebiet Kraftfahrzeugzulassungsbehörde, Hauptstraße 1, 30169 Musterhausen

Ort, Datum: Musterhausen, 12.09.2003

☒ Die gesamte Datenverarbeitung wird bei der Daten verarbeitenden Stelle selbst durchgeführt.

☐ Teile der Datenverarbeitung werden bei einem Auftragnehmer durchgeführt. Das Auftragsverhältnis ist schriftlich geregelt, § 6 NDSG wird beachtet.

Name und Anschrift der Auftragnehmer sowie Art der Datenverarbeitung (z.B. Erfassung, Mikroverfilmung, Vernichtung)

Seite 1

4. Zweckbestimmung des Verfahrens

Nachweis aller zugelassenen und vorübergehend stillgelegten kennzeichenpflichtigen Kraftfahrzeuge und Anhänger. Nachweis der natürlichen und juristischen Personen und Personenvereinigungen in ihrer Eigenschaft als Fahrzeughalter und als Inhaber von Kurzzeitkennzeichen, roten Dauerkennzeichen und Ausfuhrkennzeichen. Nachweis über die zugeteilten Ausfuhrkennzeichen und roten Dauerkennzeichen.

5. Rechtsgrundlage der Verarbeitung

§§ 31 ff. Straßenverkehrsgesetz, § 23 Straßenverkehrszulassungsordnung, Fahrzeugregisterverordnung, Verordnung über internationalen Kraftfahrzeugverkehr, Gesetz über die Pflichtversicherung für Kfz-Halter, Kraftfahrzeugsteuergesetz

6. Kreis der Betroffenen

Natürliche und juristische Personen und Personenvereinigungen in ihrer Eigenschaft als Fahrzeughalter und als Antragsteller von Kurzzeitkennzeichen, roten Dauerkennzeichen und Ausfuhrkennzeichen.

Ungefähre Anzahl der Betroffenen: ca. 70.000 registrierte Fahrzeughalter

7. Fristen für die Sperrung und Löschung der Daten

Die Sperrung und die Fristen für die Löschung von Daten richten sich nach den §§ 15 und 16 der Fahrzeugregisterverordnung

Seite 2

8.1 Art der gespeicherten Daten Jeder Betroffenenkreis ist einzeln aufzuführen; siehe auch Ausfüllhinweise	8.2 Herkunft oder Empfänger bei regelmäßiger Übermittlung Es ist anzukreuzen, ob es sich um eine übermittelnde (Ü) oder empfangende (E) Stelle handelt.		Ü	E
	a	Kraftfahrt-Bundesamt	☒	☒
	b	Finanzamt	☐	☒
	c	Haftpflichtversicherungen	☒	☒
	d	Andere Kfz-Zulassungsbehörden	☒	☒
	e	Polizeidirektion	☐	☒
	f	Straßenverkehrsbehörden (OWi-Verfolgung))	☐	☒
	g		☐	☐

	a	b	c	d	e	f	g
Vorname	x	x	x	x	x	x	
Familienname	x	x	x	x	x	x	
Geburtsname	x	x	x	x	x	x	
Geburtsdatum	x	x	x	x	x	x	
Geburtsort	x	x	x	x	x	x	
Name und Bezeichnung der juristischen Person	x	x	x	x	x	x	
Anschrift und ggf. Standort	x	x	x	x	x	x	
Beruf oder Gewerbe bei Selbständigen	x						
Wirtschaftszweig	x						
Versicherungsschlüssel und Vers.Scheinnummer	x		x		x		
Amtliches Kennzeichen	x	x	x	x	x	x	
Ausfuhrkennzeichen	x	x	x	x	x	x	
Technische Fahrzeugdaten	x	x	x				
Verwendung des Fahrzeugs, z.B.:. Taxi, Mietwagen, Mietwagen zur Vermietung an Selbstfahrer, Kraft-Omnibusse im Linienverkehr	x		x				

Bitte hier doppelklicken um eine neue Zeile einzufügen

☐ Es findet keine regelmäßige Übermittlung statt

Seite 3

8.3 Beabsichtigte Übermittlung von Daten in Staaten nach § 14 NDSG

Rechtsgrundlage für die Übermittlung
Die Übermittlung erfolgt im Einzelfall nach § 37 des Straßenverkehrsgesetzes

Zweck der Übermittlung
a) für Verwaltungsmaßnahmen auf dem Gebiet des Straßenverkehrs,
b) zur Überwachung des Versicherungsschutzes im Rahmen des Pflichtversicherungsgesetzes,
c) zur Verfolgung von Zuwiderhandlungen gegen Rechtsvorschriften auf dem Gebiet des Straßenverkehrs oder
d) zur Verfolgung von Straftaten, die im Zusammenhang mit dem Straßenverkehr oder sonst mit Kraftfahrzeugen, Anhängern, Kennzeichen oder Fahrzeugpapieren, Fahrerlaubnissen oder Führerscheinen stehen
e) zur Umsetzung des Kraftfahrzeugsteuergestzes

Behördeninterner Teil der Verfahrensbeschreibung

9. Angaben zu dem Verfahren nach Nr. 2

Bezeichnung des Verfahrens
Kraftfahrzeugzulassungsverfahren

Eingesetze Programme
OK.Vorfahrt der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)

☒ Verknüpfungen zu anderen Verfahren oder Dateien bestehen

Bezeichnung dieser anderen Verfahren oder Dateien
Microsoft-Word

10. Betriebsart des Verfahrens

☐ Stapel- (Batch-) Betrieb ☐ Dialogbetrieb

Bitte zusätzlich angeben
☒ Datenbank ☐ Tabellen-kalkulation ☒ Textver-arbeitung ☐ Manuell ☐ Sonstiges:

11. Art der Geräte
(Betriebssystemangaben ohne exakte Versionsnummern)

☒ Großrechner der Firma	Betriebssystem IBM (Datenbank DB/2)
☐ Rechner mittlerer Größe	Betriebssystem
☒ Vernetzte Arbeitsplatzcomputer	Betriebssystem Windows NT, Windows 2000, Windows XP
☐ Alleinstehende PC	Betriebssystem
☐ Sonstiges:	

☒ Datenfernübertragung ☒ Standleitung ("DDV" oder "HfD") ☒ Wählleitung mit Modem
☐ Sonstige Datenfernübertragungen

12. Übermittlungsverfahren

☐ COM-Mikrofiche-austausch ☐ Datenträger-austausch ☒ Dateitransfer mittels Datenfernübertragung ☒ Automatisiertes Abrufverfahren

13. Verfahren zur Sperrung, Löschung, Auskunftserteilung

☒ Manuelle Sperrung ☒ Automatische Sperrung ☒ Manuelle Löschung ☒ Automatische Löschung

Verfahren der Auskunftserteilung:
☒ Schriftliche Mitteilung ☐ Einsichtnahme vor Ort ☐ Sonstiges:

Seite 4

14. Technische und organisatorische Angaben nach § 7 NDSG

14.1 Bauliche Maßnahmen

☐	Grundsätzlich kein Publikumsverkehr in Räumen mit Arbeitsplatzcomputern (APC) oder Terminals.
☒	Alle Räume mit APC sind bei Abwesenheit der Bediensteten mit Sicherheitsschlössern verschlossen.
☐	Es werden nur APC eingesetzt (keine Zentralrechner wie Großrechner, Server, Mehrplatzsysteme).
☒	Alle Zentralrechner sind in einer Sicherheitszone mit zusätzlicher Zugangskontrolle untergebracht.
☐	Sicherung wichtiger mobiler Datenträger in separatem, gesicherten Archivraum oder Tresor.

14.2 Technische Maßnahmen

☒ Sicherung aller Rechner durch	☒ Passwort	☐ Magnetstreifenkarte/Chipkarte
☒	Die Begrenzung der Zugriffsrechte auf die zuständigen Bediensteten ist technisch gesichert.	
☐	Verschlüsselung bei der Speicherung und ggf. bei der Datenfernübertragung.	
☒	Protokollierung von Systemaktivitäten (z.B. Benutzer-Login).	
☒	Protokollierung des Zugriffs auf einzelne Datensätze.	
☐	Regelmäßige Auswertung der Protokolle.	

14.3 Organisatorische Maßnahmen

Die Zugriffsberechtigungen sind auf folgende Personen beschränkt:

Adminstratoren des Verfahrens, Sachbearbeiter der Kraftfahrzeugzulassungsbehörde mit aufgabenbezogenen differenzierten Berechtigungen.

Bedienstete des Sachgebietes Verkehrsordnungswidrigkeiten und der Polizeidirektion Musterhausen im Rahmen des Abrufverfahrens nach § 36 des Straßenverkehrsgesetzes.

☒ Eine Dienstanweisung zum Datenschutz ist vorhanden.

Sonstiges:

14.4 Weitere wichtige technisch-organisatorische Maßnahmen

Datenübermittlung an das Kraftfahrt-Bundesamt über das Testa-Netz. Datenübermittlung an das Finanzamt mit dem Programm ElsterFT. Datenabruf durch die Polizeidriektion Musterhausen über Standleitung.

Abruf 14, 21, 22, 42, 44, 84, 87, 88, 89, 142
Adresse 2, 152
Akte 15, 25, 42, 45, 100, 101, 144
Amtshilfe 40, 86, 148
Anonymisierung 62, 128, 142
Anrufung 11, 26, 73, 107, 108, 109, 110, 163
Archiv 25, 100, 101, 102
Aufgaben 12, 13, 18, 19, 20, 21, 22, 23, 24, 28, 29, 36, 37, 38, 50, 51, 67, 68, 69, 70, 71, 72, 75, 79, 80, 81, 84, 87, 88, 90, 94, 95, 112, 115, 116, 117, 118, 119, 147, 153, 154, 156, 158, 161, 163
Aufklärung 15, 46, 47, 77, 78, 108, 118, 155, 156
Auftrag 11, 14, 15, 16, 17, 39, 42, 50, 52, 55, 88, 96, 115, 143, 150, 162
Auskunft 8, 11, 21, 24, 25, 29, 41, 54, 78, 82, 83, 90, 95, 96, 97, 98, 99, 110, 117, 132, 148, 161
Ausland 9
Aussonderung 162
Beanstandung 30, 108, 120, 121
Berichtigung 11, 25, 54, 100, 101, 110, 162
Beschäftigte 122, 143, 144
Bestellung 3, 18, 19, 64, 67, 68, 69, 74, 146, 153, 155
Betroffene 14, 16, 22, 24, 42, 47, 53, 54, 78, 83, 87, 91, 95, 97, 98, 99, 102, 106, 107, 108, 117, 131, 156, 157, 158
Bundesdatenschutzgesetz 5
Bundesverfassungsgericht 5, 8, 9, 96
Daten 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 35, 36, 37, 39, 40, 41, 42, 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 111, 115, 117, 119, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 137, 139, 140, 141, 142, 143, 144, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165
Datensicherheit 56, 72, 73
Datenverarbeitung 8, 9, 11, 12, 15, 19, 29, 30, 37, 39, 40, 43, 44, 45, 46, 48, 49, 50, 51, 52, 54, 56, 58, 60, 62, 69, 70, 71, 75, 76, 77, 78, 80, 82, 88, 91, 93, 96, 101, 102, 103, 104, 107, 112, 117, 119, 122, 126, 148, 149, 150, 153, 154, 155, 156, 157, 163, 164
Datenvermeidung 9, 62, 70, 118
Dritte 14, 42, 44, 53, 105, 135, 149
Eigenbetriebe 13, 36, 147
Einsichtnahme 18, 23, 64, 67, 72, 92, 154, 160
Einwilligung 15, 27, 28, 30, 31, 32, 46, 47, 49, 73, 80, 91, 102, 110, 115, 122, 123, 124, 126, 128, 129, 137, 142, 144, 149, 150
Einzelentscheidung 11, 20, 82, 83, 157, 158
Empfänger 15, 18, 19, 22, 23, 24, 31, 46, 60, 63, 68, 72, 85, 90, 91, 92, 95, 96, 124, 129, 153, 155, 159, 164
Erforderlichkeit 62, 85, 86, 101, 132
Erhebung 8, 11, 19, 75, 77, 80, 108, 126, 128, 139, 155, 156
Europäische Union 5
Fernmessen 12, 32, 39, 137
Fernwirken 12, 32, 39, 137
Forschung 31, 124, 125, 128, 148
Funktionsübertragung 51
Gefahrenabwehr 98, 131, 156, 161
Gemeinde 49, 51, 76, 147, 160, 161
Gericht 8, 23, 92, 108
Gnadenverfahren 14, 37
Grundrecht 8, 9, 35, 76, 102
Integrität 9, 56, 57
Internet 2, 59, 61, 72, 74, 118, 154
Kontrolle 22, 26, 28, 29, 38, 52, 68, 70, 71, 81, 87, 107, 108, 116, 117
Landesbeauftragter 5, 12, 27, 111
Landtag 13, 27, 28, 36, 37, 108, 111, 112, 116, 117, 118, 119, 121
Löschung 11, 17, 18, 25, 52, 54, 55, 60, 63, 70, 72, 85, 100, 101, 102, 110, 136, 138, 162
Maßnahme 21, 58, 82, 108, 113
Nutzung 6, 10, 11, 20, 79, 84, 88, 91, 125, 137, 140, 152, 153, 156
Ordnungswidrigkeit 33, 49, 140, 143, 144
Organisation 17, 56, 59, 69
Personal 69, 133
Personalvertretung 68, 70, 71, 133
Personenbeziehbarkeit 62, 152
Personenbezug 43, 62, 152
Protokollierung 152
Pseudonymisierung 62
Register 18, 23, 63, 67, 74, 92, 153, 155
Rundfunkanstalten 14, 37
Schadensersatz 11, 26, 104, 110, 163
Schriftform 15, 31, 46, 47, 108, 124, 155
Speicherung 8, 11, 20, 24, 25, 32, 44, 64, 76, 78, 79, 80, 95, 96, 100, 101, 106, 123, 130, 133, 134, 135, 141, 153, 156
Sperrung 11, 18, 25, 52, 54, 63, 72, 100, 102, 110, 162
Stelle 8, 13, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 30, 31, 32, 35, 36, 37, 39, 42, 43, 44, 45, 47, 49, 50, 51, 52, 53, 54, 60, 61, 63, 64, 65, 67, 68, 69, 71, 73, 74, 75, 76, 79, 80, 81, 82, 84, 85, 86, 87, 88, 90, 91, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 107, 108, 109, 115, 119, 120, 121, 122, 123, 125, 127, 128, 130, 131, 133, 134, 135, 140,

141, 143, 144, 146, 149, 150, 151, 153, 154, 155, 157, 158, 160, 161, 162, 163, 164, 165
Straftat 49, 142
Tätigkeitsbericht 28, 116, 118, 119, 121
Technik 16, 53, 55, 56, 58, 61, 69, 70, 135, 150, 151
Textverarbeitung 64, 74, 146, 153, 155
Transparenz 10, 54, 57, 63, 129
Übermittlung 11, 15, 18, 21, 22, 23, 31, 41, 44, 46, 63, 72, 74, 84, 85, 86, 87, 88, 90, 91, 92, 93, 94, 105, 123, 124, 125, 127, 129, 141, 144, 146, 148, 153, 155, 158, 159, 160, 161, 163, 165
Überwachung 61, 70, 119, 131, 133, 134, 135, 152
Unabhängigkeit 38, 108, 112, 117
Unwirksamkeit 47
Veränderung 11, 17, 20, 44, 55, 60, 79, 84, 156
Verantwortung 21, 60, 84, 86, 88, 128, 164
Verarbeitung 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 30, 31, 32, 35, 36, 37, 39, 40, 41, 42, 43, 45, 46, 47, 50, 51, 53, 54, 55, 56, 57, 61, 62, 63, 64, 67, 68, 69, 70, 71, 72, 73, 74, 76, 79, 80, 81, 82, 83, 84, 87, 88, 93, 95, 96, 100, 102, 103, 104, 105, 107, 108, 109, 115, 118, 119, 122, 124, 125, 126, 127, 128, 129, 130, 134, 135, 140, 143, 144, 148, 149, 150, 151, 152, 154, 156, 157, 158, 159, 163, 164, 165
Vereinigung 37, 38, 147
Verfahrensbeschreibung 3, 11, 17, 39, 45, 63, 64, 65, 71, 132, 133, 149, 153, 167
Verfassungsschutz 6, 131
Veröffentlichung 72, 77, 128, 154, 155
Vertraulichkeit 9, 29, 56, 57, 73, 117
Verwaltungsverfahren 97
Verwaltungsvorschrift 6
Video 131
Vorabkontrolle 45, 61, 62, 69, 73, 132, 135
Wartung 51, 150
Weisung 39
Widerspruchsrecht 9, 11, 26, 103, 110, 163
Zweckbindung 8, 11, 20, 23, 40, 44, 49, 79, 80, 81, 84, 85, 88, 90, 94, 128, 129, 138, 148, 156, 160